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

2300.17
HQMC C4
27 May 2020

From: Director, IC4 Division, Deputy Commandant for Information (DC I)

Subj: MAINFRAME TERMINAL AREA SECURITY OFFICER (TASO) POLICY & PROCEDURES

Ref:
(a) MCO 5400.52
(b) DODI 8500.01
(c) DoDI 8510.01
(d) NIST SP 800-53
(e) MCO 5239.2B
(f) Computer Fraud Act of 1986
(g) 18 United States Code Chapter 47
(h) 10 United States Code Chapter 47
(i) CJCSI 6510.01F

Encl: (1) IRM- 2300.17 Mainframe Terminal Area Security Officer (TASO) Policy & Procedures

1. Purpose. To establish policy and standard processes for all Marine Corps components by identifying a set of activities, general tasks, and structure to ensure secure information systems (IS) and IT operations within the mainframe environment. This manual establishes requirements for TASO training, appointments, roles/responsibilities in system access, and termination to ensure access levels are controlled and monitored to mitigate misuse and inappropriate access to mainframe-based systems.

2. Cancellation. This document does not cancel previous policies on this topic. In accordance with applicable Marine Corps Orders (MCOs) and National Institute of Standards and Technology (NIST) Controls, this document will be reviewed annually and updated when necessary.

3. Authority. The information promulgated in this publication is based upon policy and guidance contained in references (a) through (g).

4. Applicability. This publication is applicable to the Marine Corps information systems and connecting systems.

5. Scope.

a. Compliance. Compliance with the provisions of this publication is required unless a specific waiver is authorized.

b. Waivers. Waivers to the provisions of this publication will be authorized by the Director, Information Command, Control, Communications, and Computers (IC4) Division.

6. Sponsor. The sponsor of this technical publication is DCI IC4 ICC.

L. M. MAHLOCK
BGen, USMC

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

DISTRIBUTION: PCN 18652710700

MARINE CORPS INFORMATION RESOURCES MANAGEMENT (IRM)

2300.17

MAINFRAME TERMINAL AREA SECURITY OFFICER (TASO) POLICY & PROCEDURES

June 4, 2020

Version 1.0

This page intentionally left blank

This page intentionally left blank

DOCUMENT CONFIGURATION CONTROL

Version	Release Date	Summary of Changes
Version 1.0	4 June 2020	Initial publication

This page intentionally left blank

Table of Contents

EXECUTIVE SUMMARY

This Marine Corps manual addresses the purpose, scope, role, responsibility, management commitment, and coordination for all Terminal Area Security Officers (TASOs) in the performance of their duties. This manual incorporates system access and termination requirements, as well as TASO training and appointment procedures.

This manual supports the Department of Defense (DoD) and Department of Navy (DON) directives, instructions, and policies governing cybersecurity. They are to be followed by Marine Corps commands, organizations, and detachments in applying uniform standards for the protection of Marine Corps resources that produce, process, store, and transmit information. Marine Corps Information owners are responsible for assigning a specific classification to data, while custodians (typically information systems [ISs]) design, implement, and manage appropriate controls. Clearly, defining the role of information/data owner falls upon the Commander associated with the governing authority of the Programs of Records.

This page intentionally left blank

SECTION 1.0: INTRODUCTION

Mainframe Applications access provides critical support to key business processes across the spectrum of Marine Corps functional areas, such as maintenance management, supply/logistics, manpower/military pay, and accounting/financial management. Therefore, it is vital that the Terminal Area Security Officer (TASO) program reduces the risk to these applications by following the procedures for appointment, account management, and reporting violations within execution of assigned roles and responsibilities. This manual will address the requirements for TASO training, appointments, roles/responsibilities in system access, and termination. Just as every Marine is a rifleman, every TASO must protect the network and maintain a high cybersecurity awareness posture.

1.1 Background

On 30 April 2020, the Deputy Commandant for Information (DC I) was appointed by the Secretary of the Navy (SECNAV) as the Department of the Navy Deputy Chief Information Officer (DON Deputy CIO), reference (a), and on 05 May 2020, the DON Senior Information Security Officer (SISO) appointed the Director, Command, Control, Communications, and Computers (IC4) as the DON SISO of the Marine Corps, reference (b). In accordance with MCO 5239.2B, the DON Deputy CIO shall develop, issue, validate, and maintain Marine Corps cybersecurity policies and procedures to implement cybersecurity throughout the Marine Corps and serve as the focal point for Marine Corps cybersecurity programs, tasks, standards, and prioritize cybersecurity resource requirements in the planning, programming, budgeting, and execution process for the Marine Corps software and networks.

IC4 was designated to provide leadership and governance of Marine Corps Information Management (IM) and Information Technology (IT) activities for the Marine Corps. IC4 was also tasked to oversee all planning, directing, and coordinating of IT capabilities that support Marine Corps warfighting and business functions. The Marine Corps Enterprise Network (MCEN) is the Marine Corps network-of-networks and approved interconnected network segments. It comprises people, processes, logical and physical infrastructure, architecture, topology, and Cyberspace Operations that operate according to Marine Corps policy.

The Marine Corps Mainframe Application currently reside in a hosting environment at the Defense Information Systems Agency (DISA) data center within the Mainframe Line of Business (MLOB) facility in Mechanicsburg, PA. It encompasses people, processes, logical and physical infrastructure, architecture, topology, and Cyberspace Operations that operate according to the Marine Corps policy.

1.2 Purpose

This manual establishes policy and standard processes for all Marine Corps components. IRM 2300.17 identifies a set of activities, general tasks, and structure to ensure secure information systems (ISs) and IT operations within the Mainframe environment. This manual establishes requirements for TASO training, appointments, roles/responsibilities in system access, and termination to ensure access levels are controlled and monitored to mitigate misuse and inappropriate access to Mainframe-based systems.

1.3 Applicability and Scope

1.3.1 Applicability

This manual applies to:

- Marine Corps components, organizations, and personnel (government and non-government employees) that operate aboard Marine Corps facilities or access Marine Corps IT systems. This includes any Marine Corps Mainframe Applications or networks that process, store, or transmit any Marine Corps data, whether stand alone, contractor provided, or directly connected to the MCEN backbone.
- Military personnel who may be subject to disciplinary action under the Uniform Code of Military Justice and/or criminal penalties under applicable Federal Statutes, as well as administrative sanctions if they knowingly, willfully, or negligently violate the provisions of this policy. Civilian employees and contractors are subject to criminal penalties under applicable Federal Statutes, as well as administrative sanctions if they knowingly, willfully, or negligently violate the provisions of this policy.

1.3.2 Scope

The standards identified in this manual will be used as a resource by all Marine Corps organizations and departments that acquire, develop, use, and maintain Mainframe information systems. This includes contracted third parties who use commercial devices, services, networks, and technologies in both ashore and afloat environments on the MCEN. This manual will not alter or supersede the existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence. The Intelligence Community (IC) is encouraged to respond to areas not specifically addressed by existing IC directives.

1.3.3 Objectives

The Marine Corps:

- Ensures all DoD IS and Platform IT (PIT) systems are categorized in accordance with the Committee on National Security Systems Instruction (CNSSI) 1253, reference (g).
- Implements a corresponding set of security controls from National Institute of Standards and Technology (NIST) Special Publication (SP) 800 53A and DoD-specific assignment values, overlays, implementation guidance, and assessment procedures found on Knowledge Service (KS) at https://rmfks.osd.mil.
- Protects the confidentiality, integrity, availability, authentication, and non-repudiation of Marine Corps IS, network devices, services, and technologies. As described in Department of Defense Instruction (DoDI) 8500.01 Cybersecurity, reference (d), these protections include protecting data at rest and data in transit, as well as protecting the network on which these devices operate.
- Provides training to personnel administering and maintaining Marine Corps information systems (ISs) and network devices commensurate with their duties and responsibilities.

- Supports operational effectiveness while managing risk, per DoDI 8510.01 Risk Management Framework (RMF) for DoD IT Technology, reference (e).
- Encourages interoperability between DON enclaves and DoD agencies as required, while maintaining Marine Corps security requirements outlined in this IRM.

1.4 Cancellation

This policy is the first issuance for IRM 2300.17 Mainframe TASO Policy & Procedures. Subsequent released versions will supersede this IRM as applicable.

This manual will be reviewed annually or on an as needed basis to facilitate the implementation of Access Control Policy and associated Access Controls.

1.5 Distribution

This manual is available for limited distribution to only those individuals possessing DoD Public Key Infrastructure (PKI) certificates. To request accounts, submit the requested information at https://mceits.usmc.mil/Pages/RequestAccount.aspx.

Users must provide justification for portal access. Users cannot be their own Government Point of Contact (POC). The POC should be their first-line supervisor or team lead. Users cannot list personal email addresses. Emails must be .mil or .gov accounts. To obtain access to the IRM web page, visit the Enterprise Information Technology Management (E-ITSM) IRM standards web page at https://homeport.usmc.mil/eitsm/EITSM%20Information%20Resources%20Management%20IRM%20Standar/Forms/AllItems.aspx.

1.6 Structure

This manual is organized into eight major sections: (1) Introduction, (2) Roles and Responsibilities, (3) Designating TASO, (4) TASO Responsibilities and Scope, (5) TASO Account Access Procedures, (6) Removal of TASO Rights/Privileges, (7) References, and (8) Acronyms.

1.7 Recommendations

Recommendations for changes or amendments to this manual will be submitted in writing via DONTRACKER through the DC I C4/ICC Branch at HQMC_DCI_IC4_ICC_CIO.

1.8 Effective Date

This IRM is effective upon signature of the Director IC4.

SECTION 2.0: ROLES AND RESPONSIBILITIES

The positions named in this section are responsible for the duties listed under their title.

2.1 Marine Corps IC4 Authorizing Official (AO)

The Authorizing Official (AO):

- Reviews and approves all Enterprise level Information System Security Managers (ISSM) appointments.
- Serves as oversight authority for all Mainframe Applications.

2.2 IC4 Compliance Branch/Cybersecurity

The IC4/ICC CY:

- Provides policy on the proper access and use of Marine Corps IS/IT.
- Provides risk assessment authority for the introduction or use of Marine Corps IS/IT.
- Provides policy on the proper access and use of cybersecurity and information assurance policy and standards.
- Incorporates DoD and DON policies as necessary.
- Addresses access and appropriate use issues of emerging products.

2.3 Commanding Generals (CGs)/Commanding Officers (COs)

Commanding Generals (CGs)/Commanding Officers (COs):

- Implement local procedures to comply with this manual as the final authority for access to Marine Corps Mainframe IS/IT.
- Coordinate appropriate responses to violations of site operating standards through proper channels, in accordance with (IAW) site Standard Operating Procedures (SOP).
- Ensure that only those individuals with a need-to-know are granted access to Mainframe resources.
- Appoint TASOs. TASOs must be appointed by each CG/CO, director, and officer-in-charge who has individuals in his/her organization with a requirement to have Mainframe accounts and application accesses in the performance of their duties.

2.4 Marine Corps Command Information System Security Managers (ISSMs)/Information System Security Officers (ISSOs)

Marine Corps Command Information System Security Managers (ISSMs)/Information System Security Officers (ISSOs):

- Ensure the Unit/Organization personnel follow the guidelines, processes, and procedures outlined within this manual when using the Mainframe.
- Monitor day-to-day actions conducted on the systems and network under their purview.
- Report any violation of cybersecurity standards through the proper reporting channels.
- Verify personnel requesting access to Marine Corps IS/IT have completed all required DoD, DoN, and Marine Corps Cyber Awareness training.
- Ensure all users with privileged user access to the Mainframe are appropriately trained and certified to meet the DoD 8570 requirements.

- Ensure that each Major Command using Mainframe Applications have at minimum a Primary and Alternate (Zone Level) TASO appointed in writing supporting Mainframe Application User(s).
- Ensure that each Major Supporting Command using Mainframe Applications have at minimum a Primary and Alternate (Division Level) TASO appointed in writing supporting the Mainframe Application User(s).
- Ensure that each unit using Mainframe Applications have at minimum a Primary and Alternate (Department Level) TASO appointed in writing supporting Mainframe Application User(s).
- Ensure all Mainframe TASO Appointees are familiar with the references; understand proper handling, disposal and disclosure of Personally Identifiable Information (PII); comprehend need-to-know access; and understand the gravity and ramifications of not performing appointed TASO duties and responsibilities.
- Ensure appropriate access actions (e.g., suspend, revoke, or lock) are taken on Marine Corps IS/IT accounts when personnel are dismissed, retired, separated, or transferred from the command.
- Ensure that all personnel with a Mainframe End-User Account checks out with the appointed TASO to ensure that their account and access is properly terminated prior to leaving the Command or Organization.
- Validate that the DD Form 2875 System Authorization Access Request (SAAR) form is completed in its entirety and an electronic copy is uploaded to TSO Indianapolis, IN, Mainframe hosted TASO DD 2875 (SAAR) database.
- Validate that the TASO Appointment Letter completed in its entirety and an electronic copy is uploaded to TSO Indianapolis, Indiana Mainframe hosted TASO Appointment Letter database.
- Verify all privileged users sign a Privileged Access Agreement (PAA)

2.5 The Functional Manager/Information Owners (IO)

The Functional Manager/Information Owners (IO):

- Formally appoints a system sponsor for each Automated Information System (AIS) under their cognizance.
- Establishes and publishes policies governing user access authorization to AISs under their cognizance.
- Identifies and approves all controls and safeguards which regulate the manager in which sensitive data is processed and controlled in the systems under their cognizance.

2.6 The Security Manager/Security Coordinator

The Security Manager/Security Coordinator:

- Verifies the clearance level of all personnel
- Reviews the SAAR and provide the clearance level as identified in the Joint Personnel Adjudication System (JPAS) or Defense Information Security System (DISS)

- Provides critical applications access support to key business processes across the spectrum of Marine Corps functional areas, such as maintenance management, supply/logistics, manpower/military pay, and accounting/financial management.
- Ensures the appropriate accounts are created for users and privileged users.
- Ensures system auditing is configured as required.
- Reviews log files and report anomalies to the ISSM/ISSO.
- Ensures LCSA/SYSADMIN/NETADMIN accounts are used for performing appropriate functions only and not for IS/IT application user functions.
- Retains an electronic copy of the user SAAR.

2.7 Supervisor

The supervisor:

- Evaluates and determine the user's need to know for access to the Mainframe.
- Ensures that the SAAR is properly filled out, signed, and forward the SAAR to ISSM or designated representative.

2.8 TASO

The TASO:

- Refers to section 4.0 of this manual.

2.9 Authorized Users of Mainframe Applications

The Authorized Users of Mainframe Applications:

- Ensure there is a need to know prior to accessing files or data.
- Ensure to adhere to Functional Owner/Information Owner directives, policies, and/or procedures to request and obtain program or application accesses.
- Ensure proper authorization is obtained prior to using any programs or applications.
- Restrict the use of Marine Corps Mainframe programs and applications to official use or authorized purposes only.
- Report any misuse, abuse, or other prohibited actions through the proper chain of command.
- Complete Marine Corps Cyber Awareness and Privacy training annually.
- Maintain Mainframe AccessorID (ACID)/UserID and password confidentiality by not divulging to anyone or writing them down.
- Ensure Common Access Card (CAC) is removed from the card reader when leaving the workstation.

2.10 Marine Corps Cyberspace Operations Group (MCCOG) Limited Security Control Accounts (LSCAs)

The scope and permission level of a Limited Security Control Account (LSCA) is commensurate with scope and permission level of a system administrator account. LSCA accounts are the most

trusted account level in the Mainframe Application level security structure. LSCA accounts are to be considered as privileged.

The Marine Corps Cyberspace Operations Group (MCCOG) LSCA administrators:

- Implement and enforce all DoD IS and PIT system cybersecurity policies and procedures, as defined by cybersecurity-related documentation.
- Ensure that all users have the requisite security clearances and access authorization, and are aware of their cybersecurity responsibilities for DoD IS and PIT systems under their purview before granting access to those systems.
- In coordination with the Marine Corps Mainframe Enterprise ISSM, and application ISSMs, initiate protective or corrective measures when a cybersecurity incident or vulnerability is discovered and ensure that a process is in place for authorized users to report all cybersecurity-related events and potential threats and vulnerabilities to the ISSO.
- Ensure that all DoD IS cybersecurity-related documentation is current and accessible to properly authorized individuals.
- Act as a regional cybersecurity technical advisor to the Marine Corps Mainframe Enterprise ISSM in reference to Enterprise Mainframe policy, management and development.
- Ensure each Mainframe Privileged User under their Area of Responsibility (AOR) with cybersecurity responsibilities (i.e., TASO) is appointed in writing and those appointment letters are uploaded to the Marine Corps TASO letter repository.
- Ensure that Marine Corps Mainframe Enterprise cybersecurity incidents are properly reported to the Marine Corps Mainframe Enterprise Information System Security Manager.
- Review AIS resource and ACID violations and audit records that are within their scope of authority and responsibility.
- Support all TASO and application Users under their defined scope of authority.

SECTION 3.0 DESIGNATING TASO

3.1 General

Marine Corps Commanders and Command ISSMs have a responsibility to ensure that each Major Command, Major Supporting Command, and using unit using Mainframe Applications have a primary and alternate TASO appointed in writing supporting Mainframe Application users. TASOs are the primary liaison between site personnel and the CO/ISSM. They act as the "local agent" representing the CO/ISSM at each site and adhering to the following procedures:

- All communication between site personnel and the CO/ISSM/ISSO must be done by site-appointed TASOs.
- TASOs are responsible for submitting proper and accurate request documents with all the mandatory requested information described in this instruction.

3.2 TASO Appointment

Marine Corps Organization Heads, Command Information System Security Managers (ISSM) and Information System Security Officers (ISSO) have a responsibility to ensure that each unit using Mainframe Applications have a primary and alternate TASO appointed in writing supporting the Mainframe Application users. TASOs are assigned a Security Control ACID to administer and support users who access multiple AIS hosted within the Mainframe and accessed via a secure Telnet 3270 terminal/printer emulation. TASOs ensure all personnel with a Mainframe end user account have a need-to-know, appropriate level of clearance (where applicable), and authorized access in order to access the AIS and data stores. The Unit Commander or Director must sign the TASO Appointment Letter to validate the appointment. The TASO is the Security Administrator for the respective site once appointed.
The associated Marine Corps Enterprise Mainframe Security Structure is detailed in the following graphic in **Figure 1**.

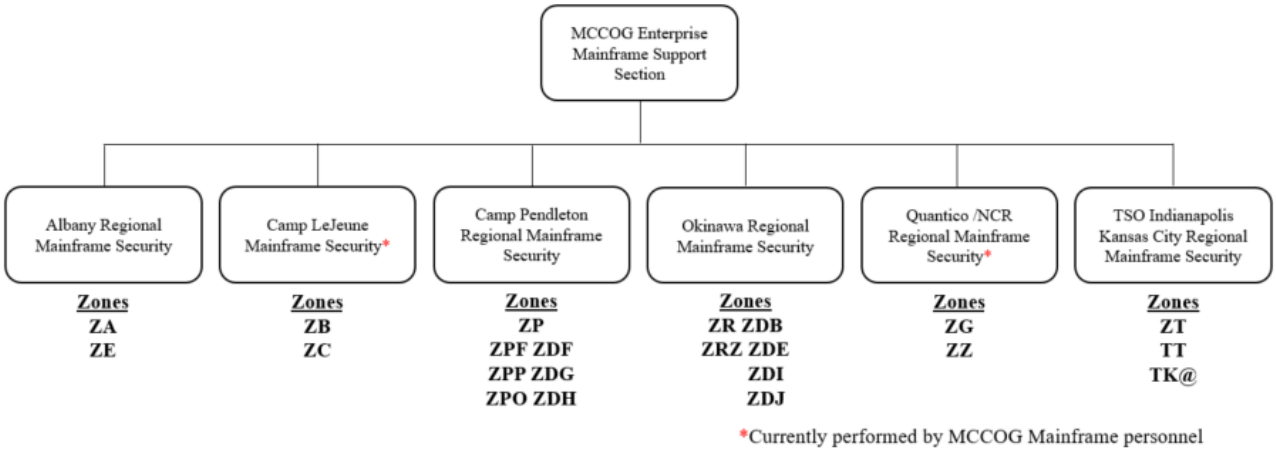

Figure 1: Marine Corps Enterprise Mainframe Security Structure

3.2.1 Regional Mainframe Security Structure

The chart, **Figure 2**, below provides an example of the Mainframe Security Structure to assist the TASO to determine the level of appointment required to administer and support the users within the Mainframe. Per this manual, each command, organization, activity or unit using Mainframe Applications must have a primary and alternate TASO appointed on each system/Logistical Partition (LPAR) they have users on.

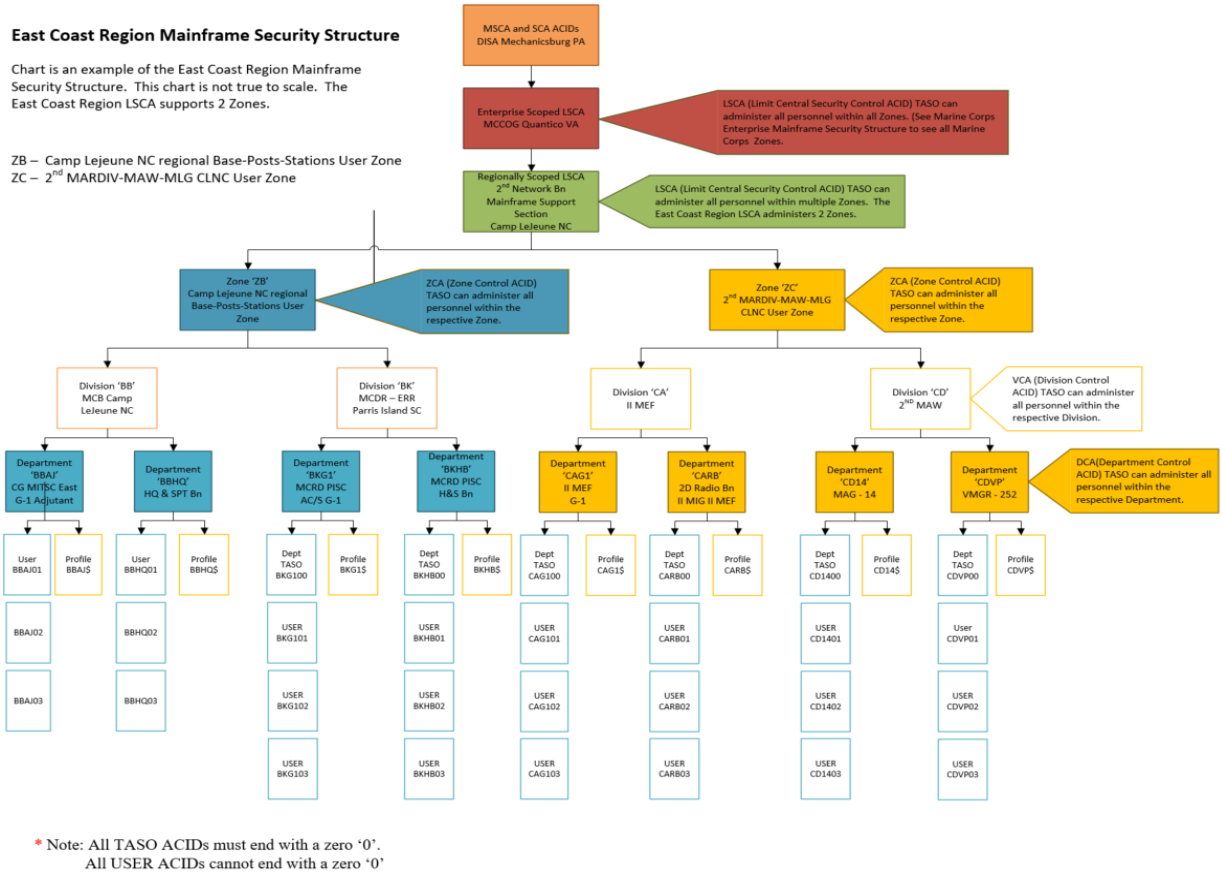

Figure 2: (EXAMPLE CHART) Regional Mainframe Security Structure

The Unit Commander/Director has the authority to submit a request appointing a new TASO.

TASOs are required to keep their LSCA, Zone, Division, and/or Department Level TASO assigned Security Control ACID active on all systems/LPARs where they have supported users. TASO status is not transferable. For example, when a user submits a Permanent Change of Active/Permanent Change of Station (PCA/PCS) for a new activity, the new activity commander must certify the need for TASO status in the job at the new location.

As with all new accounts, the TASO must log on to the system(s)/LAPRs they are appointed to support within the established time period. Exceeding 30+ days of non-use results in automatic administrative suspension, and exceeding 45+ days of non-use results in automatic deletion. Additionally, TASOs must establish a personal password and continue to access their accounts at once every 30 days. Failure to do this will result in the account being deleted. If TASO ACID is deleted, the TASO must resubmit all required documentation as an initial request for appointment and account reestablishment.

A sample of the TASO appointment letter is provided in **Appendix A**.

3.2.2 TASO Training Requirements

Access to the IS is a privilege. The privilege to access the IS requires an initial training to obtain and an annual refresher training to maintain.

3.3 Required Training for All Personnel

All Marine Corps personnel using Marine Corps IS will conduct appropriate initial or annual trainings for DoD IA/Cyber Awareness and PII. Civilians will perform training on the Total Workforce Management System (TWMS). Military and Contractor personnel will perform training on MarineNet. The DoD Information Assurance (IA)/Cyber Awareness and PII training is valid for 365 days from the day training is completed. Links to required annual training sites are listed below.

USMC Annual Security Training is available on MarineNet for Active Duty or Reserve Marines and Contractors at https://www.marinenet.usmc.mil. The same training is available on TWMS for Marine Corps Civilians at https://twms.navy.mil/login.asp. Below is a list of required trainings for all personnel:

- DoD IA/Cyber Awareness
- PII Assurance Awareness

Specific training required for TASOs can be obtained on MarineNet: https://www.Marinenet.usmc.mil/Courses/taso_final_r1/taso_index.htm.

3.4 TASO Background Investigation Requirements

DoD Military, Government Civilian personnel, consultants, and contractor personnel performing duties within the MCEN IS may be assigned to one of the position sensitivity designations and minimally investigated as followed.

1.) LSCA ACID Level TASO.

- ADP-I (IT-1): Single Scope Background Investigation (SSBI)/SSBI Periodic Reinvestigation (SBPR)/SSBI Phased Periodic Reinvestigation/(PPR)/or equivalent Tiered Investigation/T5/or Tier 5 Reinvestigation/T5R.

2.) ZONE Control AccessorId (ZCA)/Division Control AccessorId (VCA)/Department Control AccessorID (DCA) ACID Level TASOs.

- ADP-II (IT-2): Access National Agency Check with Written Inquiries (ANACI)/National Agency Check with Local Agency and Credit Checks (NACLC)/Secret Periodic Review (S-PR)/or equivalent Tiered Investigation/T3/Tier 3 Reinvestigation/T3R.
- ADP-III (IT-3): National Agency Check with Inquiries (NACI)/or equivalent Tiered Investigation/T1 or Tier 1 Reinvestigation/T1R are not eligible to be assigned as a TASO at any level.

3.) Those with a Background Investigation (BI)/National Agency Check (NAC)/Entrance National Agency Check (ENTNAC) or equivalent Tiered Investigation/T4/Tier 4

Reinvestigation/T2R or Tier 2 Investigation/T2/Tier 2 Reinvestigation/T2R are not eligible to be assigned as a TASO at any level.

3.4.1 Types of Security Administrators and their Scope of Authority

Title	Scope	Example
MSCA	Entire installation ***** DISA ONLY *****	The master SCA (MSCA) can create all CA Top Secret administrators, including SCAs, LSCAs, ZCAs, VCAs, and DCAs.
SCA	Entire installation ***** DISA ONLY *****	An SCA's scope of authority depends on the administrative authorities that they were granted. An SCA can create ZCAs, VCAs, DCAs, Profile, and User ACIDs, but not other SCAs.
LSCA	A zone and/or another LSCA ***** DFAS/MCCOG/NETWORK BN/MCLC Albany GA and TSO Indianapolis Regional Mainframe Security Personnel ONLY ******	An LSCA can have all the authority of an SCA, but unlike the SCA, the LSCA must have scope of authority assigned to it. This scope of authority can be one or more LSCAs and/or Zones.
ZCA	A zone ***** ANY MILITARY/GOVERNMENT CIVILIAN/CONTRQCTOR THAT MEETS ALL OTHER ASSIGNMENT REQUIRMENTS ******	A zone administrator can: • Permit access to resources owned by the zone, all connected divisions, departments, and users within that zone. • Define profiles and perform maintenance for ACIDs that are within scope. • Create ACIDs in the zone. • Permit ACIDs in other zone access to his zone's resources, but cannot perform maintenance for ACIDs in other zones.
VCA	A division ***** ANY MILITARY/GOVERNMENT CIVILIAN/CONTRQCTOR**	A division security administrator can: • Permit access to resources owned by the division, all departments and users within that division. • Define profiles and perform maintenance for ACIDs that are within scope.

	THAT MEETS ALL OTHER ASSIGNMENT REQUIRMENTS ****	• Create ACIDs in the division. • Permit ACIDs in other divisions access to his division's resources, but cannot perform maintenance for ACIDs in other divisions.
DCA	A department ***** ANY MILITARY/GOVERNMENT CIVILIAN/CONTRQCTOR THAT MEETS ALL OTHER ASSIGNMENT REQUIRMENTS ******	Department administrators have the same scope over a department that a VCA has over a division. DCAs can also create ACIDs in their department.

Table 1: Security Administrators and Scope of Authority

3.4.2 Limited Security Control Account (LSCA)

LSCA accounts are ADP-I (IT-I) with SSBI/SSPR/PPR/Tier 5 or T5R investigation positions. The LSCA account access is considered a privileged user account. It is a position where the incumbent is responsible for the planning, direction, and implementation of a computer security program. The major responsibility includes the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

All privileged users must undergo a Single Scope Background Investigation (SSBI) for Tier 5 regardless of security clearance level required even if no clearance or only Confidential or Secret is required.

All LSCA or Privileged Access account owners must be issued a DISA RSA SID 700 NCPASS digital token and the associated token serial number registered with the DISA Mainframe Access Control Program (ACP) on each system their LSCA TASO accounts or Privileged Access accounts reside to facilitate two-factor authentication.

3.4.3 ZONE Control ACID (ZCA)/DIVISION Control ACID (VCA)/DEPARTMENT Control ACID (DCA) Level TASOs

All ZONE, DIVISION, and DEPARTMENT Level TASO accounts are ADP-II (IT-II) with ANACI/NACLC/Tier 3 investigation positions. These position are limited privileged with non-critical sensitive access. A background investigation must be approved in accordance with the applicable government or contractor designations.

3.4.4 USER Level access

USER Level accounts will be adjudicated in accordance with the Privileged User designated requirements or the Non-Privileged User designation requirements.

USER Level accounts will be adjudicated in accordance with the Limited Privileged User designation requirements as they fall within the ADP-II (IT-II) with ANACI/NACLC/Tier 3 investigation positions for financially sensitive and/or PII sensitive designated IS/IT/Applications access permissions or the Non-Privileged User designation requirements as they fall within the ADP III (IT-III) with a Background Investigation (BI)/National Agency Check (NAC)/Entrance National Agency Check (ENTNAC) or equivalent Tiered Investigation/T4/Tier 4 Reinvestigation/T2R or Tier 2 Investigation/T2/Tier 2 Reinvestigation/T2R for those non-financially sensitive or non- PII sensitive designated IS/IT/Application access permissions. The User position is ether non-privileged with non-sensitive (low risk) or limited privileged with non-critical sensitive access. A background investigation must be approved in accordance with the applicable Military, Government or Contractor designations and meet the access sensitivity requirements of the IS/IT/Applications for which access is being requested.

SECTION 4.0: TASO RESPONSIBILITIES AND SCOPE

The TASO must:

- Ensure each Mainframe End-User has a need-to-know, appropriate level of clearance (where applicable), and authorized access in order to gain entry into the AIS and data stores.
- Confirm each Mainframe End-User is only assigned one Mainframe End-User Account. Mainframe End-User accounts are not to be shared or duplicated, per the Computer Fraud Act of 1986, Public Law 99-474. Violation of this requirement is punishable under Chapter 47 of Title 18 of United States Code and under the Uniform Code of Military justice.
- Perform the assigned security duties and responsibilities in an effective, efficient, and responsible manner. This includes management of the Mainframe Accounts under their control, and the associated initial temporary password and password resets. It is important to ensure that login credentials and password information are only provided to the authorized Mainframe Account holder via confidential and secure means. If not provided face-to-face, account credentials and password information must be sent separately via signed and encrypted email to the account holder.
- Verify the overall Mainframe Application Security posture is maintained at an acceptable level relative to DoD and Marine Corps AIS and their associated data.
- Report all security violations and inappropriate actions that could be detrimental to the overall Mainframe Application security posture to the DoD and Marine Corps AIS and their associated data stores. The LSCA/TASO is required to report this information to their IS Security personnel or chain of command as soon as recognized.
- Ensure that the authorized Mainframe Account holder’s information is correctly entered in the Security Account format as identified in the Automated Mainframe TASO Data Input Panels. Mainframe Security Account format is right-aligned and will consist of: Last Name (including suffix Sr, Jr, II, III, etc.), First Name, Middle Initial (if any, or as space allows), Military Rank irrespective of Not Pay Grade (i.e. SGT not E-5), CTR for

Contractors, and the appropriate schedule or pay band for Civilians (e.g. GS-09, YA-02, NH-III, etc.).

- All Security Accounts will have the Attribute No Automatic Terminal Sign (NOATS) on defined to the account. This is a Security Technical Implementation Guide (STIG) requirement.
- At no time will an ACID transfer with a USER from one duty station to the next duty station. Permissions granted to an ACID are not transferable.
- At no time will a USER share an ACID. ACID assignment(s) are for only the approved user associated with the approved SAAR on record.
- Ensure upon a members' departure/transfer, the subject Mainframe Account is deleted. Unused or vacant Mainframe Accounts are no longer authorized.

4.1 Administration

There are three primary administrative elements involved in the controlling and granting of access to data/information:

- User Administration.
- Functional Administration.
- Security Systems Administration.

This manual focuses on the User Administration for TASOs.

4.2 User Administration

Besides the previously listed responsibilities, the TASO who will be the Department Control Administrator (DCA), Division Control Administrator (VCA), or Zone Control Administrator (ZCA) will ensure:

- Every TASO has access via their TASO account, which must be defined on every system/LPAR he/she administers.
- Every TASO knows of every user he/she administers. A TASO cannot ensure that access criteria is being met and access credentials are properly disseminated unless he/she knows the users he/she is to administer.
- Every TASO has physical access to all spaces where his/her user gain access to IS/Applications.
- That TASOs are able to define their users to each of the systems/LPARs' TSS and grant or assist in gaining them the appropriate access permissions and authorities requested, authorized, and approved for.
- They can provide NATURAL System Security (NSS) access for their users as required, based on the appropriate access permissions and authorities requested, authorized and approved for.
- That every user will be administered in both TSS and NSS by the same Zone (ZCA), Division (VCA) or Department (DCA) TASOs appointed by their command, organization, activity or unit. The only exceptions are those access permissions that can only be administrated at the regional and/or enterprise LSCA TASO level.

Additionally, the TASO must:

- Assist the LSCA ISSOs in meeting their assigned duties and responsibilities.
- Implement and enforce DoD IS and PIT system cybersecurity policies and procedures, as defined by cybersecurity-related documentation.
- Ensure users have the requisite security clearances and access authorizations. Users must be aware of their cybersecurity responsibilities for DoD IS and PIT systems under their purview before granting access to those systems.
- In coordination with the Marine Corps Mainframe Enterprise Information System Security Manager and application ISSM, initiate protective or corrective measures when a cybersecurity incident or vulnerability is discovered. Ensure a process is in place for authorized users to report all cybersecurity-related events, potential threats, and vulnerabilities to the ISSO.
- Ensure DoD IS cybersecurity-related documentation is current and accessible to properly authorized individuals.
- Confirm Marine Corps Mainframe Enterprise cybersecurity incidents are properly reported to their respective LSCAs/ISSOs or the Marine Corps Mainframe Enterprise Information System Security Manager.
- Support all TASOs and users under your scope as defined by your ACID standard naming definition in the performance of cybersecurity related duties.
- Review/audit ACIDs for non-use (i.e. “suspend” status).
- Contact ACID owners in a “suspend” status and verify account is still required. Un-suspend/Re-activate account if appropriate.
- For ACIDs no longer required, or those owned by personnel that have departed the command, organization, activity, or unit, the account will be deleted unless the subject account is under investigation. If under investigation, the account will be brought to the attention of their respective LSCAs/ISSOs or the Marine Corps Mainframe Enterprise ISSM to ensure such ACIDS are relocated to the respective System/LPARs’ TSS ZZBRIG department.
- The departing TASO must notify their respective LSCAs/ISSOs or the Marine Corps Mainframe Enterprise ISSM of intention to depart. Upon notice, access will be terminated according to the departing/termination date.

SECTION 5.0: TASO ACCOUNT ACCESS PROCEDURES

5.1 ZONE (ZCA) Level TASO Access

The ZONE Level TASO Access Procedures are listed below:

- Successfully complete the MarineNet TASO course.
- Request a ZONE (ZCA) ACID assignment from Regional LSCA/ISSO or Enterprise ISSM.
- Complete the TASO Appointment Letter from IRM 2300.17. Appendix A: Appointment Letter and have letter signed per defined format.
- Complete a DD Form 2875 (SAAR) requesting ZONE (ZCA) TASO access permissions with justification.

- Forward the completed TASO Appointment Letter to Regional LSCA/ISSO or Enterprise ISSM for approval and subsequently uploaded to the Mainframe hosted TASO Appointment Letter database for required record keeping.
- Forward the completed DD Form 2875 (SAAR) to Regional LSCA/ISSO or Enterprise ISSM for approval and subsequently uploaded to the Mainframe hosted TASO DD Form 2875 (SAAR) database for required record keeping.

5.2 DIVISION (VCA) Level TASO Access

The DIVISION Level TASO Access Procedures are listed below:

- Successfully complete the MarineNet TASO course.
- Request a DIVISION (VCA) ACID assignment from ZONE TASO, Regional LSCA/ISSO, or Enterprise ISSM.
- Complete the TASO Appointment Letter from IRM 2300.17. Appendix A: Appointment Letter and have letter signed per defined format.
- Complete a DD Form 2875 (SAAR) requesting DIVISION (VCA) TASO Access permissions with justification.
- Forward the completed TASO Appointment Letter to Regional LSCA/ISSO or Enterprise ISSM for approval and subsequently uploaded to the Mainframe hosted TASO Appointment Letter database for required record keeping.
- Forward the completed DD Form 2875 (SAAR) to Regional LSCA/ISSO or Enterprise ISSM for approval and subsequently uploaded to the Mainframe hosted TASO Appointment Letter database for required record keeping.

5.3 DEPARTMENT (DCA) Level TASO Access

The DEPARTMENT Level TASO Access Procedures are listed below:

- Successfully complete the MarineNet TASO course.
- Request a DEPARTMENT (DCA) ACID assignment from the DIVISION, ZONE, Regional LSCA/ISSO, or Enterprise ISSM.
- Complete the TASO Appointment Letter from IRM 2300.17. Appendix A: Appointment Letter and have letter signed per defined format.
- Complete a DD Form 2875 (SAAR) requesting DEPARTMENT (DCA) TASO access permissions with justification.
- Forward the completed TASO Appointment Letter to Regional LSCA/ISSO or Enterprise ISSM for approval and subsequently uploaded to the Mainframe hosted TASO Appointment Letter database for required record keeping.
- Forward the completed DD Form 2875 (SAAR) to Regional LSCA/ISSO or Enterprise ISSM for approval and subsequently uploaded to the Mainframe hosted TASO Appointment Letter database for required record keeping.

5.4 User Access Requirements

Access to IS/IT and/or Applications is essential to the Marine Corps mission. To ensure all personnel that access the Mainframe understand their responsibilities where this risk is

concerned, there is a requirement for all personnel to read, complete, and digitally sign the SAAR. Requestor's Portion, blocks 1 through 15, and the USMC DD 2875 Addendum Standard Mandatory Notice and Consent Provision for all DoD Information Systems.

SECTION 6.0: REMOVAL OF TASO RIGHTS/PRIVILEGES

6.1 Commands

Normally, a TASO appointment remains in effect until that TASO ACID owner is formally relieved by the appointment of another Zone (ZCA), Division (VCA) or Department (DCA) TASO.

In the event that a TASO ACID owner is suspected of knowingly, willfully, or negligently violate the provisions of this policy the Regional LSCA/ISSO or Enterprise ISSM must be notified as soon as possible to ensure such ACIDs are relocated to the respective System's/LPARs' TSS ZZBRIG department for safekeeping until such time that an investigation is conducted and completed.

6.2 TASO Account Establishment Documents Guidance and Instructions

Step 1 – How to identify a TASO Control ACID for TASO Appointment

- Control ACIDs are used for administrative purposes and define security administrators that are associated with various structural levels within the Mainframe security structure. Department Control ACID (DCA), Division Control ACID (VCA), and Zone Control ACID (ZCA) are types of Control ACIDs assigned to TASOs. **A 6-character ACID ending in zero (0) identifies a Control ACID. At no time will a TASO Control ACID end in numerical characters 1-9 or alphabetical characters A-Z.**
- A TASO Control ACID at each level Zone (ZCA), Division (VCA) or Department (DCA) TASO will be determined by next higher echelon TASOs and provided to the Requestor.
- Once a Requestor has been provided a TASO Control ACID, he or she can proceed to Step 2.

Step 2 – MarineNet TASO Distance Learning Course

- The TASO Distance Learning Course provides the necessary job-related background information and skills in two Mainframe software security applications; Broadcom Inc. CA-TSS and Software AG. NATURAL Security Services (NSS) to allow students to perform the duties of a TASO.
- Open Internet Explorer and launch MarineNet: https://www.marinenet.usmc.mil/MarineNet/Home.aspx
- When prompted, select your PKI CAC authentication certificate, and click OK.
- Read the US DoD warning statement, and click AGREE when complete.
- Within the MarineNet home page search engine, enter TASO.
- Click the VIEW/ENROLL icon for course "Terminal Area Security Officer (TASO) (0688AO0000)."
- Click ENROLL to reach My Active Courses.

- Click LAUNCH for course code 0688AO0000.
- Click LAUNCH Course to begin. See **Figure 3** for landing page view.
- Complete all lessons within the TASO Course and take the Final Practice/Test.

Figure 3: TASO Course Landing Page

- After completion of the TASO Course and Final Practice Exercise/Test, two documents will be produced:
  1. TASO Course Completion Certificate.
  2. TASO Appointment Letter (Use appointment letter from IRM 2300.17 for most updated version).

Step 3 – Complete DD Form 2875 – SAAR

The Requestor will initiate a SAAR for TASO privileges by completing the blocks as listed below. Scanned or hand written SAARs are **NOT** accepted. The SAAR process is 100% electronic/digital. The only version of the SAAR accepted for TASO appointment can be accessed using the below link. Copy and Paste within your Internet browser to launch. Ensure to request access, if prompted. HQMC DC I, IC4 URL: https://www.hqmc.marines.mil/Portals/137/Docs/Info%20Systems%20Mgt/NIPR%20User%20SAAR%20190917.pdf

It is recommended the Requestor completes the SAAR as instructed within this guidance to ensure accuracy of the form.

Instructions for Requestor

Type of Request = check the **INITIAL** block (*no other option will be accepted*).

User ID = Enter the Control ACID provided by Zone TASO, Division TASO, or Department TASO Mainframe Security Administrator within the available field. **A six (6) character ACID ending in zero (0) identifies a Control ACID. At no time will a control ACID end in numerical characters 1-9 or alpha characters A-Z.** (*EDIPI is not accepted in this field)*

Date = Date of request being initiated.

System Name = MSB, MSF, and/or MSI TASO. (*No other system names will be accepted*)

ONLY ENTER THE SYSTEMS THAT USERS REQUIRE ACCESS TO

Location = Mechanicsburg, PA.

Block 1 NAME = Requestor's Official LAST NAME (*with suffix if applicable*), FIRST NAME, MIDDLE INITIAL (*i.e. Smith Jr, John P.*).

Block 2 ORGANIZATION = Requestor's Major Command/Major Supporting command/Unit Name. *(USMC will NOT be accepted)*

Block 3 OFFICE SYMBOL/DEPARTMENT = Requestor's platoon code or office code (*e.g. G-1*).

Block 4 PHONE = Requestor's official work phone number.

Block 5 OFFICIAL EMAIL ADDRESS = Requestor's military email address.

Block 6 JOB TITLE AND GRADE/RANK = Requestor's billet, grade AND rank. (*e.g. Administration Specialist, Cpl/E4*)

Block 7 OFFICIAL MAILING ADDRESS = Requestor's official command mailing address.

Block 8 CITIZENSHIP = Requestor's citizenship.

Block 9 DESIGNATION OF PERSON = Specify if Requestor is Military, Civilian, or Contractor.

Block 10 IA TRANING AND AWARENESS CERTIFCATION REQUIREMENTS = Block 10 will be marked with an 'X' Cyber Awareness training must be within the last 12 months and verified via the Requestor training certificate. Marines-MarineNet CYBERM000, Civilian-TWMS Cyber Awareness, Contractor-MarineNet CYBERC.

Block 13 JUSTIFCATION = an example of an acceptable TASO appointment justification is provided below.

> *Requests appointment as the 'command' or 'ZONE, DIV, or DEPT name' TASO. Typical duties include, but not limited to: Validation/Verification of personnel who have a need-to-know; Mainframe Application access Policies and Procedures, Mainframe Security*

rules, User Administration; ACID creation/assignment; ACID deletion; Review/Update/Assist personnel within appointed scope for name change, grade/rank changes, and/or federal service change; Password resets; ACID suspension/un-suspension.

An example of 'command' is '2D MARDIV' or '2ND BN 8TH MARINES'

An example of ZONE 'C Zone' NAME = '2ND MARDIV-MAW-MLG CLNC ZONE'

An example of DIV 'CE Division, NAME = '2D MARDIV DIV'

An example of DEPT 'CEG1 Department' NAME = 'G-1 2ND MARDIV DEPT'

Addendum Pages: Requestor must read and digitally sign SAAR addendum.

Block 12 DATE = Requestor can leave this block blank; however if utilized, the date must match the digital signature date in block 11.

Block 11 USER SIGNATURE = Requestor must digitally sign this block.

Requestor will electronically forward the SAAR to immediate supervisor. Supervisor will complete the SAAR blocks as listed below.

Instructions for Supervisor

Block 14 TYPE OF ACCESS REQUIRED = Supervisor must mark this block "**AUTHORIZED**".

Block 15 USER REQUIRES ACCESS = Supervisor must mark this block "**UNCLASSIFIED**".

Block 16 VERIFICATION OF NEED TO KNOW = Supervisor must mark this block with an "X."

Block 16a ACCESS EXPIRATION DATE = This block is reserved for use by contractor employees.

Block 17 SUPERVISOR'S NAME = Supervisor's full LAST NAME (*with suffix if applicable*), FIRST NAME, MIDDLE INITITAL (*i.e. Smith Jr, John P.*) and must include their Grade/Rank.

Supervisor must be a SNCO, Officer or GS-06 or above and senior to the REQUESTOR.

Block 20 SUPERVISOR'S ORGANIZATION/DEPARTMENT = Supervisor's command. *(USMC will NOT be accepted)*

Block 20a EMAIL ADDRESS = Supervisor's military email address.

Block 20b PHONE NUMBER = Supervisor's official work phone number.

Block 19 DATE = Supervisor can leave this block blank, however, if utilized, the date must match the digital signature date in block 18.

Block 18 SUPERVISOR'S SIGNATURE = Supervisor must digitally sign this block.

Leave blocks 21-25 blank. These are for the Regional and Enterprise Mainframe LSCA TASOs/ISSOs/ISSMs action only.

The Requestor is responsible to ensure the Supervisor completes the SAAR blocks as outlined above before proceeding. Upon completion of Supervisor SAAR blocks, the SAAR must be electronically forwarded to the command Security Manager. The Security Manager will complete blocks 28-32.

Instructions for Security Manager

Block 28 TYPE OF INVESTIGATION = At a minimum, the investigation requirement is a favorably completed and adjudicated Tier 3/Tier 3R/T3investigation for military, civilian, and contractor personnel. A clearance is NOT required for TASO Appointment; however a favorably adjudicated investigation is required. ANACI or NACLC adjudicated investigations will still be accepted until they are phased out. **(Tier 1) or NACI investigations are insufficient and will not be accepted.**

Block 28a DATE OF INVESTIGATION = Security Manager must populate date of investigation completion/adjudication.

Block 28b CLEARANCE LEVEL = If the background investigation has a favorable adjudication, indicate 'Favorable,' level of clearance granted (e.g. Secret, Top Secret, SSBI, etc.), or eligibility. "N/A," "OPEN," "SCI," "Pending," "No Determination Made," or "Interim" are NOT acceptable terms referencing an adjudication.

Block 28c IT LEVEL DESIGNATION = This block is not required to be marked. **IT LEVEL III** will not be accepted if marked.

Block 29 VERIFIED BY = Security Manager must mar his name as the responsible party who verified the Requestor's background information. Must match name in block 31.

Block 30 SECURITY MANAGER TELEPHONE NUMBER = Security manager's official work phone number.

Block 32 DATE = This block can be left blank, however, if utilized, the date must match the digital signature date in block 31.

Block 31 SECURITY MANAGER SIGNATURE = Security Manager must digitally sign this block.

The Requestor is responsible for ensuring the Security Manager completes blocks 28-32 as outlined above before proceeding.

If blocks 28-32 are completed as outlined above, proceed to Step 5.

Step 4 – Submitting the TASO Account Establishment Documents for Processing

Requestor Instructions

If requestor is attached to the MCEN, the below is the ONLY authorized means to submit for TASO appointment.

Contact your respective Regional or Enterprise Mainframe Customer Support LSCA TASO/ISSOs or ISMM if requestor is NOT attached to the MCEN for submission instructions.

1) Requestor must have the below paperwork completed as outlined within this guidance prior to completing this step.

- MarineNet TASO Appointment Letter.

Please not the Appointment Letter from MarineNet is outdated. To obtain the most updated version of the TASO appointment letter see IRM 2300.17 Appendix A.

- TASO DD FORM 2875 (SAAR).
- Cyber Awareness Certificate.

Marines- MarineNet CYBERM0000, Civilian- TWMS Cyber Awareness, Contractor- MarineNet CYBERC

The Cyber Awareness course certificate completion date and SAAR Block 10 date MUST match.

2) Requestor will contact command S-6 or G-6 Authorized Submitter, also known as an ISC or CTR, to initiate a service request using Enterprise Remedy System. Most Authorized Submitters are unfamiliar with Mainframe TASO requests. Therefore requestor should provide the Authorized Submitter the instructions listed on the next page.

3) Requestor will provide Authorized Submitter required paperwork to initiate the request.

- TASO Appointment Letter
- TASO DD Form 2875 (SAAR)
- Cyber Awareness Certificate.

4) Requestor is responsible to follow up with the Authorized Submitter to ensure service ticket is opened/initiated.

5) Requestor is responsible to review Enterprise Remedy email notifications for status pertaining to TASO Appointment. Check junk mail for all Enterprise Remedy email notifications.

The Authorized Submitter must then take action.

Authorized Submitter Instructions

1) Authorized Submitter should have received the below documents from the requestor to initiate the service request for a Mainframe TASO account:

- TASO Appointment Letter.
- TASO SAAR.
- Cyber Awareness Certificate.

2) Authorized Submitter must initiate a service request via Enterprise Remedy Service Request Management (SRM) on behalf of the requestor. Authorized Submitter does not

validate the SAAR, nor validate training requirements for Mainframe TASO accounts. Authorized Submitter does NOT complete blocks 22-25 of the Requestor SAAR.

3) Select CREATE USER ACCOUNT.

4) Within the Create User Account template, the following fields must be completed, as listed below, to ensure the work order is routed correctly for processing.

- Unit/Command S-6 Authorized Submitter will open service ticket "on Behalf of" *{search and select the Requestor's name}* to update the "Requested for" name. All personnel requiring support must have a People Record in the correct Organizational Unit (OU).
- Network Classification = MCEN-N {NIPR Marine Corps Network}.
- Account Type = *Other/Not Listed.*
- Account Description = *Mainframe TASO Account.*
- Did you attach the documentation required for your request? Check "YES" if Requestor provided required documentation. Attach required forms. If required forms are NOT provided to the Authorized Submitter, the 'Create User Account' request cannot be entered/submitted.
- Account Details =Authorized Submitter will Enter *'Route to appropriate Regional Mainframe Customer Support Enterprise Remedy Queue for action. TASO Account Request'*

The Requestor will be notified when appointment is effective through the Marine Corps Enterprise Service Desk Enterprise Remedy System. Requestor is responsible to review Enterprise Remedy email notifications for status pertaining to TASO Appointment. It is advised to check junk mail for all Enterprise Remedy email notifications.

A User Account Screenshot is available below, **Figure 4**.

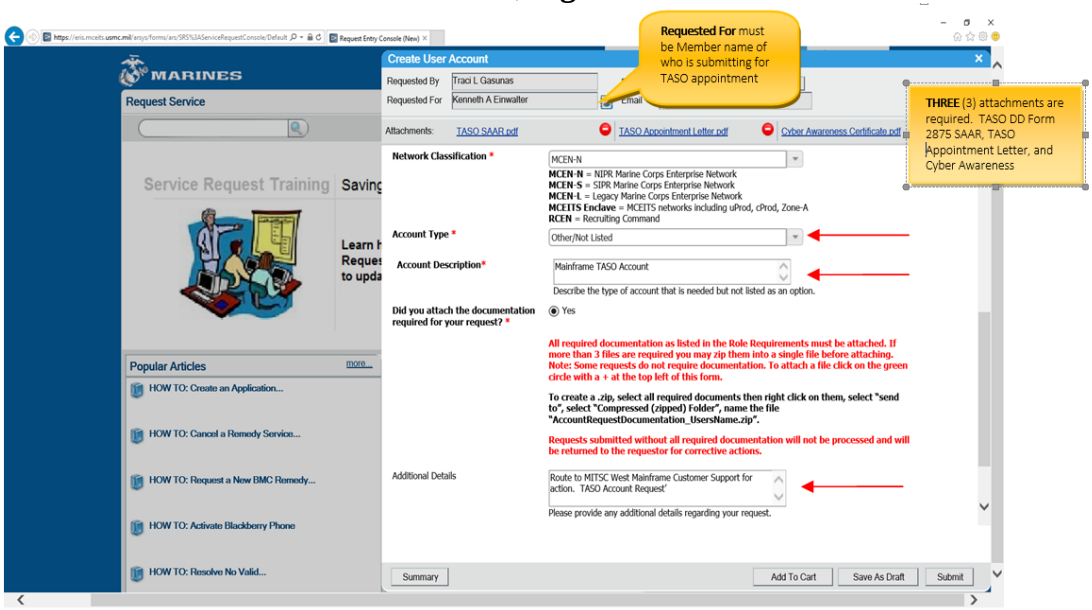

Figure 4: User Account Screen

SECTION 7.0: REFERENCES

7.1 Publications

This section provides a list of relevant statutes, regulations, directives, and other guidance applicable to IT security in order of reference in this manual. It includes those cited in this document as well as other items that concerned personnel might need to understand. Although it is not a comprehensive collection of IT security-related references and authorities, it is sufficiently detailed to facilitate the reader's use of this document and to understand other IT security-related documentation.

- SECNAV Memo, Designation of the Department of the Navy Deputy Chief Information Officer (Navy) and the Department of the Navy Deputy Chief Information Officer (Marine Corps), 30 April 2020
- DON SISO Memo, Designation of the Department of the Navy Deputy Senior Information Security Officer (Navy) and the Department of the Navy Deputy Senior Information Security Officer (Marine Corps), 5 May 2020
- MCO 5400.52, Department of the Navy (DON) Deputy Chief Information Officer Marine Corps Roles and Responsibilities, 5 January 2010
- DoDI 8500.01, Cybersecurity, 14 March 2014
- DoDI 8510.01, Risk Management Framework (RMF) for DoD IT Technology (IT), 12 March 2014
- Applicable Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs)
- Applicable NIST SP 800-53 control requirements

7.2 Other Publications

This section provides a list of other publications that have relevance to this IRM, but were not directly referenced within the document.

- MCO 5239.2B, Marine Corps Cybersecurity, 05 November 2015
- Computer Fraud Act of 1986, Public Law 99-474
- 18 United States Code Chapter 47, Fraud and False Statements, 04 January 1995
- 10 United States Code Chapter 47, Uniform Code of Military Justice, 07 January 2011
- CJCSI 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," 10 October 2013

7.3 Marine Corps IRMs Website

The IRMS are located at:
https://homeport.usmc.mil/eitsm/EITSM%20Information%20Resources%20Management%20IRM%20Standar/Forms/AllItems.aspx.

SECTION 8.0: ACRONYMS

ACID	Accessor ID
ADP	Automated Data Processing
AIS	Automated Information System
AOR	Area of Responsibility
CAC	Common Access Card
CNSSI	Committee on National Security Systems Instruction
DISA	Defense Information Systems Agency
DJMS	Defense Joint Military Pay System
DoD	Department of Defense
EDIPI	Electronic Data Interchange Personal Identifier
IA	Information Awareness
LSCA	Limited Security Control Account
MCCOG	Marine Corps Cyberspace Operations Group
MCEN-N	NIPR Marine Corps Network
NIPR	Non-classified Internet Protocol Router
PCS	Permanent Change of Station
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIT	Platform IT
PKI	Public Key Infrastructure
SAAR	System Authorization Access Request
SASO	Special Actions Security Office
SRP	SASO Request Package
STIG	Security Technical Implementation Guide
TA	Trusted Agent
TASO	Terminal Area Security Officer
TDY	Temporary Duty
ZCA	Control AccessorID
VCA	Division Control AccessorID
DCA	Department Control AccessorID (DCA)
ZZBRIG	Holding zone for accounts pending investigation

APPENDIX A: APPOINTMENT LETTER FORMAT

UNITED STATES MARINE CORPS
Unit Letter Head

Today's Date

From: ***OIC/Supervisor***

To: ***Your name [FIRSTNAME MI. LASTNAME Suffix/EDIPI/rank or grade]***

Subj: **APPOINTMENT AS TERMINAL AREA SECURITY OFFICER (TASO)**

Ref:

(a) MSGID/GENADMIN/CMC WASHINGTON DC C4 CY/1709-01/SEP17

(b) Computer Fraud and Abuse Act of 1986

1. You are hereby appointed as a (***Division or Department***) TASO for (***div or dept***). You are to thoroughly familiarize yourself with references (a) and (b). This appointment will remain in effect until you are formally relieved by the appointment of another (***Division or Department***) TASO.

2. You are assigned the TASO account of ***ACID account*** for _____.

3. You will carry out the TASO duties of maintaining accounts in your (***Division or Department***) ensuring that they are being used or deleted and suspended. This will be in compliance with the rules and regulations set by DISA and the Marine Corps.

OIC's Signature _____

OIC's Name: ***OIC Name (type), Title***

****

FIRST ENDORSEMENT

From: ***Your name [LASTNAME Suffix, FIRSTNAME MI./EDIPI/rank or grade]***

To: ***OIC Name (type), Title***

Subj: **TASO APPOINTMENT LETTER**

1. I have read and understand references (a) and (b) and have assumed all duties in conjunction with my appointment as a (***Division or Department***) TASO.

2. My duty phone number is Comm: **XXX-XXX-XXXX** and/or DSN: **XXX-XXX**__.

TASO's Signature _____
TASO's Name: ***Your name (type)***