



UNITED STATES MARINE CORPS
MARINE FORCES RESERVE
2000 OPELOUSAS AVE
NEW ORLEANS, LOUISIANA 70114-5400

ForO 5270.1
G-6

FORCE ORDER 5270.1

From: Commander
To: Distribution List

Subj: INFORMATION SYSTEMS COORDINATOR AND PRIVILEGED USER PROGRAM

Ref: (a) Marine Corps Information Enterprise Strategy Implementation
Planning Guidance Version 1.1
(b) Force Order 3440.1H
(c) MARADMIN 175/15: MCBUL 5210 E-Mail Usage Policy
(d) DoDD 8140.01 "Cyberspace Workforce Management" 11 August 15
(e) MSG 150049Z JUN 13 Next Generation Enterprise Network
Information Systems Coordinator Program
(f) Force Order 5239.2
(g) MITSC-Res ISC Procedures
(h) ECSD_024 Cybersecurity Workforce Improvement Program

Encl: (1) Information Systems Coordinator/Privileged User Duties and
Training
(2) DD Form 2875 System Authorized Access Request
(3) Privileged Access Authorization Request
(4) Tool Access Request
(5) Appointment/Relief Letters and Endorsements
(6) Turnover Desktop Procedures
(7) USMC Regional Service Desk Contact Information

1. Situation. The Marine Corps Next Generation Enterprise Network (NGEN) solution returned control of the Marine Corps Enterprise Network (MCEN) to a Government-Owned, Government-Operated (GOGO) environment. As such, Marine Forces Reserve (MARFORRES) must ensure it has a sufficiently staffed, trained, and certified workforce to provide Information Technology (IT) services for all MARFORRES users.

a. This Order provides guidance and direction for the appointment, training, and equipping of Information System Coordinators (ISC) and Privileged Users. ISCs can consist of communication personnel and non-communication personnel capable of providing on-site services to local commands and to support MARFORRES voice, video, and data networks. Note that as part of NGEN, there are contractors dispersed throughout MARFORRES who will also assist in managing the network and providing support to MARFORRES. Command ISCs and Privileged Users are all part of the Cybersecurity Workforce (CSWF).

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

b. Per references (a) through (h) and as part of the Marine Corps' transition from Navy Marine Corps Intranet (NMCI) to NGEN, MARFORRES, Major Subordinate Command (MSC) staff, and individual units/sites will develop a CSWF. This workforce will play an enhanced role in providing support for the operation and maintenance of all MARFORRES managed networks. The workforce will provide IT services that are essential to facilitating mission accomplishment for all users. This added responsibility is due to the Marine Corps assuming full control of its networks and the loss of contract labor associated with the NMCI network. Without an accredited workforce, users on all MARFORRES networks will experience a significant reduction with End User Service (EUS) deskside support. Requesting new services, also known as Request fulfillment, will also be negatively impacted due to longer wait times from a centralized service model.

c. The transition from NMCI to the MCEN affects all units down to each Home Training Center (HTC). During this transition, it is critical that commands identify the right personnel to assist users with IT support. Personnel performing the duties as a basic ISC will not have administrative privileges on the network; instead, ISCs will train users, troubleshoot basic issues, liaise with the local service desk, perform data calls, and disseminate policy. Many hours of specialized training and certifications are required before an individual can be assigned as a Privileged User. Privileged Users are granted permissions that allow them to make changes on the network; without proper training, those privileges could have a negative impact on users across the force. Personnel who qualify and are approved by their commands will be granted administrator privileges and must adhere to the CSWF requirements in references (d), (f), and (h). Privileged Users will receive permissions to local machines and/or critical troubleshooting tools in order to better support the delivery, installation, operation, and maintenance of IT services to users within their command. Both Privileged Users and ISCs are permitted access to the USMC Remedy trouble ticketing system to better facilitate incident management and request fulfillment within their scope of responsibility.

2. Mission. MARFORRES, MSC staff, and all Inspector-Instructor (I-I) staffs will identify, facilitate training, and maintain a viable workforce of ISCs and Privileged Users (where feasible) in order to provide flexible, timely, and reliable data and phone service support at all MARFORRES sites.

3. Execution

a. Commander's Intent

(1) Purpose. The purpose of the ISC and Privileged User program is to establish an onsite capability to serve as a user's first-response for IT support.

(2) Method

(a) MARFORRES G-6 will formalize the ISC and Privileged User program and ensure each MSC and I-I staff possesses the ability to request services, resolve IT-related problems, and facilitate the efficient management of all MARFORRES networks.

(b) MARFORRES G-6 will centrally manage all networks, facilitate IT requests, and manage resolution of problems that are escalated from subordinate MSC or I-I staff ISCs.

(c) The MARFORRES G-6 Regional Service Desk (RSD) will facilitate the restoration of services, synchronize regional IT processes, use automated network management and service delivery tools to reduce the potential burden levied on local ISCs, and ensure problems are logged in a common database in a consistent manner.

(d) MSC G-6s will actively participate in the oversight and development of the ISC program. ISCs will work with their Major Subordinate Elements (MSE) to ensure best practices and coordinate with joint I-Is to best support the unique reserve structure.

(e) Command S-6, I-I staff S-6, and ISCs will adhere to all policy and procedures developed by MARFORRES G-6, serve as first responders for IT requests within their organizations, and escalate any problems/issues they are unable to resolve to the MSC G-6 and/or MARFORRES RSD.

(f) Privileged Users will be incorporated down to the lowest element where resources allow. They should be relied upon to perform tasks that are complex in nature and require elevated privileges on the MCEN. ISCs should continue to improve their skills where less reliance on the Privileged Users and the MARFORRES RSD is required. This will allow faster response times and better support to the end user.

(g) MSC and I-I Privileged Users will only be granted those permissions required to support their staff in order to mitigate potential unintended impacts to the enterprise network.

(3) End-state. MARFORRES possesses a trained workforce of ISCs and Privileged Users who provide onsite support at each location to assist MARFORRES, MSC, and I-I staff by providing flexible, timely services to every command.

b. Concept of Operations

(1) Scheme of Maneuver. New ISCs will be appointed in writing and complete all required training per references (c), (d), (f), and (h). MARFORRES staff, Commanding Generals, and I-Is will maintain eligible ISCs at each site where the unit maintains a presence. All

appointed individuals must complete their required training as identified in enclosure (1) of this Order. ISCs must submit completed System Access Authorization Requests (SAAR), per enclosure (2) of this Order. Eligibility requirements are listed in paragraph 3.d.1 of this Order. ISCs will become familiar with their IT environments. In addition to the requirements of ISCs, Privileged Users will also complete the Privileged Authorized Access Request (PAAR), enclosure (3), and Tool Access Request (TAR), enclosure (4). Privileged User eligibility requirements are listed in paragraph 3.d.2 of this Force Order. The requirements for the CSWF are summarized for the ISC and Privileged Users in enclosure (1) in accordance with (IAW) reference (d).

c. Tasks

(1) MARFORRES G-6

(a) Implement and manage the Force ISC and Privileged User Program.

(b) Develop policy and manage the processes for the ISC and Privileged User program.

(c) Facilitate training and process requests for elevated permissions.

(d) Manage the list of appointed ISCs and Privileged Users throughout MARFORRES.

(e) Facilitate the submission and tracking of trouble tickets electronically via the Remedy ticketing system. In cases where the ISC and Privileged User does not have a Remedy account, facilitate the submission of tickets verbally at the lowest level possible via the next senior ISC or Privileged User.

(f) Monitor process compliance and identify ISCs or Privileged Users who may require additional training or supervision.

(g) Ensure the ISCs and Privileged Users are kept informed of current issues and developments in Tactics, Techniques and Procedures (TTP).

(2) MSC Assistant Chief of Staff, G-6

(a) Ensure all ISCs and Privileged Users meet eligibility requirements described in paragraph 3.d of this Order.

(b) Screen and upload signed appointment letters, training certificates, SAAR, and PAAR forms to the trackers identified in paragraph 4.a.1.

(c) Ensure all ISCs and Privileged Users request access to the Remedy ticketing system per enclosure (4), TAR form. Assist ISCs with TAR request issues.

(d) Ensure all ISCs and Privileged Users are kept informed of current issues and developments in TTP. Monitor ISC performance and training.

(e) Retain digital copies of ISC/Privileged User appointment letters, SAARs, and PAARs.

(f) Create a chain of coordination for remote sites so ISCs will know whom to contact for support.

(3) Headquarters Battalion and MARFORRES Staff Sections

(a) Ensure all ISCs and Privileged Users meet eligibility requirements described in paragraph 3.d of this Order.

(b) Assign, in writing, a primary ISC. Alternate ISCs are encouraged but not mandated. A sample Appointment letter is available in enclosure (5).

(c) Ensure ISCs and Privileged Users complete all required training per enclosure (1) IAW reference (d).

(d) Upload signed Appointment letters, Training certificates, SAAR and PAAR forms to the trackers located in paragraph 4.a.1.

(4) Commanding Officers and Inspector-Instructors

(a) Ensure all ISCs and Privileged Users meet eligibility requirements described in paragraph 3.d of this Order.

(b) Assign, in writing, a primary ISC at each site on which a unit maintains a presence. Alternate ISCs are encouraged but not mandated. A sample appointment letter is available in enclosure (5).

(c) Submit signed appointment letters, training certificates, and SAARs to the RSD, MARFORRES G-6, via the MSC G-6.

(d) Ensure ISCs and Privileged Users complete all required training and follow all guidance from MARFORRES G-6.

(e) Assign a replacement and/or alternate ISC prior to the primary ISCs departure.

(5) Information Systems Coordinator and Privileged User

(a) Complete required authorized access requests and Training certifications. Submit signed appointment letters and completed Training certifications to MARFORRES G-6 via the MSC G-6.

(b) Assist end users with Incident Management and Request fulfillment matters as required.

(c) Coordinate with the MSC G-6 when attempting to resolve issues beyond local capability and/or training. Use the appropriate chain of coordination to resolve issues at the lowest level first.

(d) Complete training and submit a TAR form for Remedy access.

(e) Submit and track all requests and incident response actions via Remedy.

(f) Participate in weekly ISC and Privileged User teleconferences IAW paragraph 5.b.4.

(g) Perform duties IAW assigned tier group and guidance provided within enclosure (1) and reference (g).

(h) Obtain an Information Technology Procurement Review/Approval System account as required. Consult with your S-6 or the next S-6 in your chain of command for additional guidance.

(i) Provide unit orientation for the logical layout of your network and the priorities of your command so that NGEN contractors can provide knowledgeable support to your area. Assist authorized contractors who are dispatched to your location in order to provide support to your command.

(j) Create and maintain Turnover Desktop Procedures IAW enclosure (6). Desktop Procedures provide a daily guide for your duties and will facilitate continuity of service if you are temporarily out of office or when you transition from the command.

d. Coordinating Instructions. Appointment letters indicate Command approval for individuals with appropriate permissions to serve as an ISC.

(1) The eligibility requirements for a basic ISC:

(a) Any Military Occupational Specialty (Marine, Navy, civilian, or contractor).

(b) E-3 through O-3. Exceptions will be considered on a case-by-case basis.

(c) Demonstrate an aptitude for understanding IT.

(d) Demonstrate an aptitude for customer service.

(e) Complete A+ Essentials 2012 (Marine Net Code: AP220801) within six months of assuming the position.

(f) Review and comply with Marine Air-Ground Task Force Information Technology Support Center - Reserves (MITSC-Res) ISC Procedures located in reference (g).

(g) Submit a TAR form for Remedy access, enclosure (4).

(h) Possess a Secret clearance (interim is acceptable).

(2) The eligibility requirements for a Privileged User:

(a) All of the requirements for a basic ISC.

(b) Complete Security+ and earn Security+ certificate, required for (.S) Admin.

(c) Complete A+ or Net+ and earn certificate, required for (.W) Admin.

(d) Submit a TAR form for Remedy access, enclosure (4).

(e) Information Assurance Policy and Technology certificate required.

(3) Membership in the CSWF does not exclude the individual from being assigned as an ISC. However, personnel who are members of the CSWF are fully qualified to execute ISC duties and provide an additional level of technical expertise needed to resolve IT issues. Generally, CSWF personnel are taken from military occupational specialties identified as 06XX, 28XX, 595X, 26XX, 29XX, etc., which have an understanding of, and training on, information systems and technology. Consideration should be given to the size and scope of the organization in order to determine how many ISCs should be assigned to assist the Privileged Users.

(4) Units located on Marine Corps installations will contact the service desk of their host installation for Incident Management support. The help desk numbers for Marine Corps installations are located in enclosure (7).

4. Administration and Logistics

a. Administration

(1) Submit appointment letters, proof of training, SAAR, and PAAR to the RSD via the following link:
<https://sharepoint.marforres.usmc.mil/G6/SitePages/Home.aspx>.

(2) The MARFORRES ISC portal can be accessed via the following link: <https://sharepoint.marforres.usmc.mil/G6/MITSC/process/ISC>.

(3) Submit TAR forms to the respective MSC G-6 IAW enclosure (4).

(4) Incident Management is defined as response to a problem or outage on the network.

(5) Request Fulfillment is defined as a Request for Information (RFI), Request for Service (RFS), or Request for Assistance (RFA). It is something the user needs. ISCs can service RFIs, but RFS and RFA must be completed by Privileged Users or MITSC-Res RSD personnel.

(6) Network Support is defined as any action necessary to maintain the functionality of the network.

b. Logistics. Training and permissions. Several effective and relevant training venues are available to potential ISCs at NO COST to the individual or the government. All required training can be found online at Federal Virtual Training Environment, Marine Net, and the MARFORRES SharePoint site. These courses provide the opportunity for Privileged Users to obtain the required training and ISCs to obtain additional training without significant impact to their primary duties. A detailed list of required training courses is found in enclosure (1).

5. Command and Signal

a. Command. An ISC chain of coordination is established to facilitate the efficient and timely submission of ISC packages as well as resolution of problems at the lowest level. Units with more capable or highly trained personnel are free to assist subordinate units in troubleshooting and resolving issues. However, the chain of coordination DOES NOT preclude direct coordination between MSC G-6 and MARFORRES G-6 in order to resolve service interruptions and outages.

(1) This Order is applicable to all MARFORRES units.

(a) ISC Communications Chain of Coordination is:

1. MARFORRES G-6.
2. MSC G-6.
3. Inspector-Instructor (MSE).
4. Inspector-Instructor (unit).

b. Signal

(1) This Order is effective the date signed.

(2) The MARFORRES RSD can be contacted at (504)697-7777.

(3) Direct technical questions regarding the implementation of the Force ISC program to MARFORRES ISC Manager at OMB: MITSC_RES_ISC or MITSC.RES.ISC@usmc.mil.

(4) For access to the weekly ISC telephone conferences contact the MARFORRES ISC Manager at OMB: MITSC_RES_ISC or MITSC.RES.ISC@usmc.mil.

(5) Updates to ISC and Privileged User contact information are to be submitted to the MARFORRES ISC Manager at OMB: MITSC_RES_ISC or MITSC.RES.ISC@usmc.mil.

(6) Contact your MSC G-6 for items not specifically covered by this Order.



REX C. MCMILLIAN

DISTRIBUTION: D

Directives issued by this Headquarters are published and distributed electronically.

Information System Coordinator/Privileged User Duties and Training

ISC Basic (no advanced permissions)	Privileged User (elevated permissions)
<p style="text-align: center;"><u>Required MINIMUM Qual/Certs</u></p> <ul style="list-style-type: none"> • Annual Cyber Awareness Training • A+ Essentials 2012 (MarineNet Code: AP220801) • MITSC-Res ISC Procedures • Remedy training <p style="text-align: center;"><u>Permission Groups</u></p> <ul style="list-style-type: none"> • Standard User Access 	<p style="text-align: center;"><u>Required MINIMUM Qual/Certs</u></p> <ul style="list-style-type: none"> • All ISC training requirements • IAT Level 1 - A+ Certification or Network+ Certification required for .W account • IAT Level 2 - Security+ Certification Required for .S account • Remedy training • Information Assurance Policy and Technology (IAP&T) Certificate required. Training located at: http://iaseapp.disa.mil/eta/iapt_v5/index.htm <p style="text-align: center;"><u>Permission Groups</u></p> <ul style="list-style-type: none"> • Desktop Administrator • Workstation Local Administrator
<p style="text-align: center;"><u>ISC Basic Tasks</u></p> <ul style="list-style-type: none"> • Coordinate all efforts within the ISC chain of coordination • Assist users with learning all automated office productivity tools • Submit user trouble tickets electronically via the Remedy ticketing system • Provide users with updated status of their trouble tickets from the Remedy ticketing system • Assist user in receiving assistance from the MFR helpdesk and service desk • Assist the MFR G-6/CTR team with issues relating to NGEN directives • Assist MFR G-6/CTR team with the 	<p style="text-align: center;"><u>Privileged User duties include all previous ISC Basic tasks as well as the following, depending on permissions group</u></p> <ul style="list-style-type: none"> • Add and remove machines from the domain - .S • Add and remove software - .W • Make changes in Active Directory (create and rename computers) - .S • Add local printer - .W • Perform local administrator functions as directed - .W • Work tickets to resolve issues as needed - .W or .S • Install end-user HW/SW at the user location, including connecting Office of Designated

<p>tech refresh process</p> <ul style="list-style-type: none"> • Submit Request for Service Remedy tickets • Coordinate planned physical seat relocations with the MFR G-6 Service Desk/CTR team • Act as the POC for seat modifications • Inform the MFR G-6 Service Desk/CTR team when users are added or removed, and create Remedy ticket 	<p>Approving Authority (ODAA) approved peripherals - .W or .S</p> <ul style="list-style-type: none"> • Install Host-Based Security System Agents and Modules that cannot be installed by remote mechanisms - .W • Install patches that cannot be remediated by remote mechanisms - .W • Remote into machines to aid users in troubleshooting problems - .W <p>.W = Workstation admin account .S = Server admin account</p>
<p style="text-align: center;"><u>ISC Basic Tasks, continued</u></p> <ul style="list-style-type: none"> • Assist Unit S-6 as a POC to MFR G-6 Service Desk • Assist users with CAC/Reader issues • Assist users with PKI certificate issues • Assist Unit S-6 with video and telephone conferencing • Assist users with all service-wide messaging systems • Assist MFR G-6 CSWF Section with response to a cybersecurity incident • Assist users with the application self-help menu • Assist with the inventory of all IT assets • Assist with the execution of the AIRS 405/630 Checklist • Maintain an ISC Turnover folder with desktop procedures • Maintain ISC eligibility requirements • Provide support for unclassified and classified services. NIPR and SIPR Remedy access required • Post all ISC documents to the ISC webpage on the MFR portal • Troubleshoot connectivity issues • Locate systems in support of Computer Network Defense (CND) 	<p style="text-align: center;"><u>MSC/S6/SvD Tier II/FS Reps</u></p> <p style="text-align: center;"><u>Required MINIMUM Qualifications/Certifications</u></p> <ul style="list-style-type: none"> • Security+ OR GSEC OR SSCP • Applicable O/S and CE Qualification <p style="text-align: center;">-----</p> <p style="text-align: center;"><u>Tasks</u></p> <ul style="list-style-type: none"> • Hardware installation/removal • Software installation/removal • Rename machines • Assign IPs • Add/remove machines from domain • Remote into machines to aid users in troubleshooting problems <p style="text-align: center;">-----</p> <p style="text-align: center;"><u>Permission Groups</u></p> <ul style="list-style-type: none"> • Desktop Admin • Workstation Local Admin

investigations

- Report suspicious activity to the MITSC-Res RNOSC
- Troubleshoot software
- Assist in correcting Base Area Network/Local Area Network (BAN/LAN) issues when directed
- Assist in providing adjustments to (BAN/LAN) infrastructure when directed
- Assist in troubleshooting and repairing Layer 2 and 3 devices (routers, switches, etc.) when directed
- Counsel users for unauthorized activity
- Map network printers to the new end-user computer, in cases where the end-user computer is being replaced
- Provide access to migrated data or external data storage devices to ensure end-user data sources are valid and available

ISC Basic Tasks, continued

- Ship, via registered mail, or as specified by DoD 5000.2-R if classified, the media (or entire device, if required) within 48 hours to the Government POC
- Furnish end-user support of Data At Rest (DAR) services, to include hard disk data recovery if full-disk encryption DAR services cause a failure
- Serve as POC to RNOSC-RES and MFR G-6 Network Admin for site degradation and outages
- Repair or swap broken hardware / replace hard drives
- Reimage computer workstations
- Provide onsite resources to manage end-user HW installation processes, including troubleshooting issues after

<p>delivery and installation of end-user HW</p> <ul style="list-style-type: none">• Perform local administrator functions as directed by MFR G-6 helpdesk or service desk• Submit NIPR and SIPR Remedy tickets on behalf of users• Troubleshoot incident management issues• Coordinate all efforts within the ISC chain of coordination• Dispose of IT equipment• Destroy, or coordinate for destruction various media that may contain PII or classified information upon determination that said media is to be disposed of	
--	--

DD Form 2875 System Authorized Access Request

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)			
PRIVACY ACT STATEMENT			
AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form. ROUTINE USES: None. DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.			
TYPE OF REQUEST <input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID			DATE (YYYYMMDD)
SYSTEM NAME (Platform or Applications)		LOCATION (Physical Location of System)	
PART I (To be completed by Requestor)			
1. NAME (Last, First, Middle Initial)		2. ORGANIZATION	
3. OFFICE SYMBOL/DEPARTMENT		4. PHONE (DSN or Commercial)	
5. OFFICIAL E-MAIL ADDRESS		6. JOB TITLE AND GRADE/RANK	
7. OFFICIAL MAILING ADDRESS		8. CITIZENSHIP <input type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER	9. DESIGNATION OF PERSON <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) <input type="checkbox"/> I have completed Annual Information Awareness Training. DATE (YYYYMMDD)			
11. USER SIGNATURE		12. DATE (YYYYMMDD)	
PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)			
13. JUSTIFICATION FOR ACCESS			
14. TYPE OF ACCESS REQUIRED: <input type="checkbox"/> AUTHORIZED <input type="checkbox"/> PRIVILEGED			
15. USER REQUIRES ACCESS TO: <input type="checkbox"/> UNCLASSIFIED <input type="checkbox"/> CLASSIFIED (Specify category) <input type="checkbox"/> OTHER			
16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. <input type="checkbox"/>		16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)	
17. SUPERVISOR'S NAME (Print Name)	18. SUPERVISOR'S SIGNATURE	19. DATE (YYYYMMDD)	
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT	20a. SUPERVISOR'S E-MAIL ADDRESS	20b. PHONE NUMBER	
21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER	21b. DATE (YYYYMMDD)	
22. SIGNATURE OF IAO OR APPOINTEE	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE (YYYYMMDD)

DD FORM 2875, AUG 2009

PREVIOUS EDITION IS OBSOLETE.

Adobe Professional 8.0

26. NAME (Last, First, Middle Initial)			
27. OPTIONAL INFORMATION (Additional information)			
<p>By signing block 11 I agree to the following rules of behavior:</p> <ul style="list-style-type: none"> - I understand that I am providing both implied and expressed consent to allow authorized authorities, to include law enforcement personnel, access to my files and e-mails which reside or were created on Government IT resources. - I will not conduct any personal use that could intentionally cause congestion, delay, or disruption of service to any Marine Corps system or equipment. - I will not install or use any Instant Messaging client or peer-to-peer file sharing application, except that which has been installed and configured to perform an authorized and official function. - I will not use Marine Corps IT systems as a staging ground or platform to gain unauthorized access to other systems. - I will not create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings, regardless of the subject matter. - I will not use Government IT Resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation. - I will not use Government IT resources for personal or commercial gain without commander approval. These activities include solicitation of business services or sale of personal property. - I will not create, download, view, store, copy, or transmit materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited such as transmitting sexually explicit or sexually oriented materials. - I will not use Marine Corps IT systems to engage in any outside fund-raising activity, endorse any product or service, participate in any lobbying activity, or engage in any prohibited partisan political activity. - I will not post Marine Corps information to external newsgroups, bulletin boards or other public forums without proper authorization. This includes any use that could create the perception that the communication was made in ones official capacity as a Marine Corps member, unless appropriate approval has been obtained or uses at odds with the Marine Corps mission or positions. - I will not use Marine Corps IT resources for the unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data. - I will not modify or attempt to disable any anti-virus program running on a Marine Corps IT system without proper authority. - I will not connect any personally owned computer or computing system to a DoD network without prior proper written approval. 			
PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION			
28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION (YYYYMMDD)	
28b. CLEARANCE LEVEL		28c. IT LEVEL DESIGNATION	
NATO Date: <input type="text"/>		<input type="checkbox"/> LEVEL I <input type="checkbox"/> LEVEL II <input type="checkbox"/> LEVEL III	
29. VERIFIED BY (Print name)	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE (YYYYMMDD)
PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION			
TITLE:	SYSTEM	ACCOUNT CODE	
	DOMAIN		
	SERVER		
	APPLICATION		
	DIRECTORIES		
	FILES		
	DATASETS		
DATE PROCESSED (YYYYMMDD)	PROCESSED BY (Print name and sign)	DATE (YYYYMMDD)	
DATE REVALIDATED (YYYYMMDD)	REVALIDATED BY (Print name and sign)	DATE (YYYYMMDD)	

DD FORM 2875 (BACK), AUG 2009

Reset

INSTRUCTIONS

The prescribing document is as issued by using DoD Component.

A. PART I: The following information is provided by the user when establishing or modifying their USER ID.

- (1) Name. The last name, first name, and middle initial of the user.
- (2) Organization. The user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).
- (3) Office Symbol/Department. The office symbol within the current organization (i.e. SDI).
- (4) Telephone Number/DSN. The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.
- (5) Official E-mail Address. The user's official e-mail address.
- (6) Job Title/Grade/Rank. The civilian job title (Example: Systems Analyst, GS-14, Pay Clerk, GS-5)/military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.
- (7) Official Mailing Address. The user's official mailing address.
- (8) Citizenship (US, Foreign National, or Other).
- (9) Designation of Person (Military, Civilian, Contractor).
- (10) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.
- (11) User's Signature. User must sign the DD Form 2875 with the understanding that they are responsible and accountable for their password and access to the system(s).
- (12) Date. The date that the user signs the form.

B. PART II: The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

- (13). Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.
- (14) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters, or settings.)
- (15) User Requires Access To: Place an "X" in the appropriate box. Specify category.
- (16) Verification of Need to Know. To verify that the user requires access as requested.
- (16a) Expiration Date for Access. The user must specify expiration date if less than 1 year.
- (17) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.
- (18) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.
- (19) Date. Date supervisor signs the form.
- (20) Supervisor's Organization/Department. Supervisor's organization and department.
- (20a) E-mail Address. Supervisor's e-mail address.
- (20b) Phone Number. Supervisor's telephone number.

(21) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.

(21a) Phone Number. Functional appointee telephone number.

(21b) Date. The date the functional appointee signs the DD Form 2875.

(22) Signature of Information Assurance Officer (IAO) or Appointee. Signature of the IAO or Appointee of the office responsible for approving access to the system being requested.

(23) Organization/Department. IAO's organization and department.

(24) Phone Number. IAO's telephone number.

(25) Date. The date IAO signs the DD Form 2875.

(27) Optional Information. This item is intended to add additional information, as required.

C. PART III: Certification of Background Investigation or Clearance.

(28) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).

(28a) Date of Investigation. Date of last investigation.

(28b) Clearance Level. The user's current security clearance level (Secret or Top Secret).

(28c) IT Level Designation. The user's IT designation (Level I, Level II, or Level III).

(29) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.

(30) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.

(31) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.

(32) Date. The date that the form was signed by the Security Manager or his/her representative.

D. PART IV: This information is site specific and can be customized by either the DoD, functional activity, or the customer with approval of the DoD. This information will specifically identify the access required by the user.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO. Recommend file be maintained by IAO adding the user to the system.

DD 2875 ADDENDUM
STANDARD MANDATORY NOTICE AND CONSENT PROVISION
FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

- You consent to the following conditions:

- o The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

- o At any time, the U.S. Government may inspect and seize data stored on this information system.

- o Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

- o This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests—not for your personal benefit or privacy.

- o Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

- Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

- The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and

User Signature Required:

data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

o In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (Le., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

o All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

User Signature Required:



Privileged Access Authorization Request**PRIVILEGED ACCESS AUTHORIZATION
REQUEST (PAAR)****PLEASE READ ENTIRELY BEFORE FILLING THIS OUT.**

INSTRUCTIONS: SAAR and PAAR forms should be submitted via the G-6 SharePoint Portal at:
<https://sharepoint.marforres.usmc.mil/G6/SitePages/Home.aspx>

Block A.

All fields in Block A are required Fields.

**ADDITIONAL DOCUMENTS TO BE ATTACHED/INCLUDED
WITH PAAR:****Block B.**

All requests for permissions in Block B should be commensurate with the Billet, Rank, Certification, Skill Set and Command of the requestor. Information System Coordinator (ISC) should refer to the ISC LOI for further guidance and pre-requisites.

PAAR Enclosures Required:

- (1) 8570 Certificate (6 Month Waiver upon approval by Cyber Security)
- (2) Cyber Security Work Force Letter
- (3) Annual Cyber Awareness Training Certificate completed less than one year from account request
- (4) Privileged-Level Access Agreement (PAA)
- (5) SAAR for new Administrative account
- (6) Privileged User IA Responsibilities (DODPUR0001)
http://iaseapp.disa.mil/eta/priv_user_ia_resp/lesson1/module.htm
Or MarineNet (Search DODPUR0001)

Administrator Privileges:

Requestor Selects the Specific Administrative Privileges Required for their billet. NOTE: MCEN-N Means NIPR, MCEN-S Means SIPR, MCEN-NL Means RNET.

(1) User Justification: Requestor must provide verbiage explaining the requirement for each level of access being requesting.

(2) Requestor's Signature: The Privileged Access Authorization Request Form must be digitally signed.

Additional Requirements for ISCs:

- (1) A+ Essentials 2012 MarineNet Certificate
- (2) ISC Appointment Letter

(3) Supervisor's Signature: Request must be approved and digitally signed by the requestor's supervisor.

(4) MSC's Signature: Request must be approved and digitally signed by the requestor's MSC when applicable. Comments should be annotated in Block 8.

(5) Cyber Security CSWIP Validation: A Member of the Cyber Security Team will validate the requestor's CSWIP compliance (Cyber Security WorkForce Letter, 8570, Annual Cyber Awareness Certificate) with regard to the requested access and billet. Non-compliance should be annotated in Block 8.

(6) MITSC Ops Approval: MITSC Ops will make the recommendation to request access, limited access, or deny the request entirely. Will verify appropriate paperwork is also attached/ included (A+ Essentials, ISC Appointment Letter, SAAR submission). Limited or no access granted should be annotated in Block 8.

(7) MITSC-Res Director's Approval: The MITSC-Res Director will review and forward the request to the G-6 for final approval and endorsement. Comments should be annotated in Block 8.

(8) Approving Chain Comments: This Space is Reserved for Comments or Recommendations by Those in the Approving Chain.

**WHEN SUBMITTING THIS PAAR, ENSURE A
CORRESPONDING DD2875 ADM SAAR IS ON FILE IN THE
SAAR TRACKER.**

PRIVILEGED ACCESS AUTHORIZATION REQUEST					
NOTE: AN APPROVED DD2875 SAAR MUST BE ON FILE BEFORE YOUR PRIVILEGED ACCOUNT CAN BE CREATED. SEE INSTRUCTIONS FOR DETAILS.					
Block A. Name:					
MSC:	Unit	City, State			
Job Title / Billet:					
Phone:			Email:		
Request Type:	<input type="radio"/> New	<input type="radio"/> Modification	<input type="radio"/> Deactivation	Date	

Block B. Privileged access is requested for the following accounts:

	MCEN-S	MCEN-N	MCEN-NL	Whiteline	N/A
Workstation (.w)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
Server (.s)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
Level IV*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
TACACS	<input type="checkbox"/>				
BigFix	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
LANSweeper	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
ISE	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>
DNS Admin			<input type="checkbox"/>		<input type="checkbox"/>
GPO Editor			<input type="checkbox"/>		<input type="checkbox"/>
Enterprise Admin			<input type="checkbox"/>		<input type="checkbox"/>
CCX			<input type="checkbox"/>		<input type="checkbox"/>
Unity			<input type="checkbox"/>		<input type="checkbox"/>
Call Manager			<input type="checkbox"/>		<input type="checkbox"/>
ACAS	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>
SCCM	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>
Domain Administrator			<input type="checkbox"/>		<input type="checkbox"/>
HBSS	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>
SQL Database	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
Other:	<input type="checkbox"/>				
If a .w or .s is account is requested:					
MITSC-Res (.mit)	<input type="checkbox"/>				
MSC G-6 (.bps)	<input type="checkbox"/>				
ISC (.tsc)	<input type="checkbox"/>				
*=Requires MCNOSC PAA					

1. User Justification For Access			
2. Requestor Signature		3. Supervisor Signature	
4. MSC Approval:		5. Cyber Security CSWIP Validation:	
<input type="checkbox"/> Concur with Requested Rights		<input type="checkbox"/> IAT Level I <input type="checkbox"/> IAT Level II <input type="checkbox"/> IAT Level III	
<input type="checkbox"/> Limited Rights Granted		<input type="checkbox"/> IAM Level I <input type="checkbox"/> IAM Level II <input type="checkbox"/> IAM Level III	
<input type="checkbox"/> No Access Granted		<input type="checkbox"/> IASAE I <input type="checkbox"/> IASAE II <input type="checkbox"/> IASAE III	
MSC Signature		Cyber Security Rep. Signature	
6. MITSC Ops Rep. Approval:		7. MITSC Dir. Approval:	
<input type="checkbox"/> Concur with Requested Rights		<input type="checkbox"/> Concur with Requested Rights	
<input type="checkbox"/> Limited Rights Granted		<input type="checkbox"/> Limited Rights Granted	
<input type="checkbox"/> No Access Granted		<input type="checkbox"/> No Access Granted	
MITSC Ops Rep. Signature		MITSC Dir. Signature	
8. Approving Chain Comments:			

MITSC-RES FORM 2875 Revision 3.5 Date: 20141014

**PRIVILEGED-LEVEL ACCESS AGREEMENT
ACCEPTABLE USE POLICY (AUP)**

**PRIVILEGED-LEVEL ACCESS AGREEMENT (PAA) & ACKNOWLEDGEMENT OF
RESPONSIBILITIES**

_____ (INITIALS) I understand that I have access to **classified and unclassified network** Marine Forces Reserve Information System (IS), and that I have and will maintain the necessary clearances and authorizations for privileged-level access to (*specify what IS privileges are being granted*).

As a privileged-level user;

_____ (INITIALS) I will protect the **root, administrator, or superuser** account(s) and authenticator(s) to the highest level of data or resource it secures.

_____ (INITIALS) I will **NOT** share the **root, administrator, or superuser** account(s) and authenticator(s) entrusted for my use.

_____ (INITIALS) I am responsible for all actions taken under my account and understand that the exploitation of this account would have catastrophic effects to all networks for which I have access. I will **ONLY** use the special access or privileges granted to me to perform authorized tasks or mission related functions. I will only use my privileged account for official administrative actions.

_____ (INITIALS) I will not attempt to "hack" the network or connected ISs, subvert data protection schemes, gain, access, share, or elevate permissions to data or ISs for which I am not authorized.

_____ (INITIALS) I will protect and label all output generated under my account to include printed materials, magnetic tapes, external media, system disks, and downloaded files.

_____ (INITIALS) I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of system or network services, illegal or improper possession of content or files, or the actual or possible compromise of data, files, access controls, or systems to the Cyber Security Officer.

_____ (INITIALS) I will **NOT** install, modify, or remove any hardware or software (i.e. freeware/shareware, security tools, etc.) without permission and approval from Cyber Security Officer.

_____ (INITIALS) I will not install unauthorized or malicious code, backdoors, software (e.g. games, entertainment software, instant messaging, collaborative applications, etc) or hardware.

_____ (INITIALS) I am prohibited from obtaining, installing, copying, pasting, modifying, transferring or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade-secret, or license agreements.

_____ (INITIALS) I will not create or elevate access rights of others; share permissions to ISs for which they are not authorized; nor allow others access to IS or networks under my privileged account.

_____ (INITIALS) I am prohibited from casual or unofficial web browsing and use of email while using the privileged-level account. This account will NOT be used for day-to-day network communications.

_____ (INITIALS) I am prohibited from accessing, storing, processing, displaying, distributing, transmitting and viewing material that is; pornographic, racist, defamatory, vulgar, hate-crime related, subversive in nature, or involves chain letters, spam, or similarly related criminal offenses such as encouragement of criminal activity, or violation of State, Federal, national, or international law.

_____ (INITIALS) I am prohibited from storing, accessing, processing, sharing, removing, or distributing Classified, Proprietary, Sensitive, Privacy Act, and other protected or privileged information that violates established security and information release policies.

_____ (INITIALS) I am prohibited from promoting partisan political activity, disseminating religious materials outside an established command religious program, and distributing fund raising information on activities, either for profit or non-profit, unless the activity is specifically approved by the command (e.g. command social-event fund raisers, charitable fund raisers, etc).

_____ (INITIALS) I am prohibited from using, or allowing others to use, Marine Corps resources for personal use or gain such as posting, editing, or maintaining personal or unofficial home pages, web-blogs, or blogging sites, advertising or solicitation of services or sale of personal property (e.g. eBay) or stock trading.

_____ (INITIALS) I am prohibited from employing, using, or distributing personal encryption capabilities for official electronic communications. I will contact the Cyber Security Office if I am in doubt as to any of my roles, responsibilities, or authorities.

_____ (INITIALS) I understand that all information processed on ISs is subject to monitoring. This includes E-mail and Web Browsing.

_____ (INITIALS) I will obtain and maintain required certification(s) in accordance with Marine Corps policy to retain privileged level access.

_____ (INITIALS) I understand that failure to comply with the above requirements is a violation of the trust extended to me for the privileged access roles and may result in any of the following actions:

- a. Chain of command revoking IS privileged access and/or user privileges
- b. Counseling
- c. Adverse actions under the UCMJ and/or criminal prosecution
- d. Discharge or Loss of Employment
- e. Revocation of Security Clearance

User Acknowledgement

NAME: _____

CAC DOD EDI Personal Identifier (EDIPI) (10 digit #): _____

SIGNATURE: _____ Date: _____

Cyber Security Endorsement

CYBER SECURITY OFFICER: _____

IA MANAGER SIGNATURE: _____ Date: _____

**PRIVILEGED-LEVEL ACCESS AGREEMENT
ACCEPTABLE USE POLICY (AUP)
CERTIFICATE OF NON-DISCLOSURE
Disclosure of protected or privileged information.**

Whoever, being an officer, employee or agent of the United States or of any department, agency or contractor thereof, publishes, divulges, discloses or makes known in any manner or to any extent not authorized by law, any information coming to him/her in the course of their employment or official duties, which information concerns or relates to the trade secrets or proprietary information of a non-Federal government entity; any information protected by the Privacy Act; any information subject to protection under the Freedom of Information Act; other law, regulation, or policy (including all privileged communications such as doctor-patient, attorney-client, etc.); any information protected under the classification system set forth in DODi 5239.1; or any other information protected by law or regulation (i.e. IG, AAA, CID); shall, in addition to any penalty imposed by said law or regulation, be subject to UCMJ, administrative, or contract remedy enforcement.

CERTIFICATION

I have read the provisions herein and I understand my responsibility not to disclose any matters connected with or pertaining to these provisions as they pertain to the Marine Forces Reserve network, except to persons theretofore listed as having a need to know.

Name: _____

CAC DOD EDI Personal Identifier (EDIPI) (10 digit #): _____

Signature: _____ Date: _____

Tool Access Request

Enterprise Remedy IT Service Management Tool Access Request Form			
Name (Last, First, MI) <input style="width: 90%;" type="text"/>	Email <input style="width: 90%;" type="text"/>		
Organization <input style="width: 90%;" type="text"/>	Job Title <input style="width: 90%;" type="text"/>		
Department <input style="width: 95%;" type="text"/>			
Address <input style="width: 95%;" type="text"/>		Status Type <input style="width: 90%;" type="text"/>	
City <input style="width: 25%;" type="text"/>	State <input style="width: 5%;" type="text"/>	Zip Code <input style="width: 20%;" type="text"/>	Request Type <input style="width: 90%;" type="text"/>
Phone Number <input style="width: 25%;" type="text"/>	Date of Request <input style="width: 20%;" type="text"/>	<input type="checkbox"/> NGEN Contractor	
Role Identification			
Primary Role <input style="width: 95%;" type="text"/>			
Please see Access Request Form instructions for Role descriptions and additional guidance on Role Identification			
Secondary Role <input style="width: 95%;" type="text"/>			
Tertiary Role <input style="width: 95%;" type="text"/>			
Before additional Roles are selected, please read and understand the guidance concerning multiple roles within the instructions			
Additional Requirements			
<input style="width: 95%;" type="text"/>			
<small>Add any Support Group requirements, Functional Roles, Application Permissions or other special requirements.</small>			
<input type="checkbox"/> NIPRNet		<input type="checkbox"/> SIPRNet	
Date <input style="width: 15%;" type="text"/>	Requestor Signature <input style="width: 90%;" type="text"/>		
Please select an Organizational Approver from the drop-down below, before signing.			
Organizational Approver			
Name (Last, First, MI) <input style="width: 90%;" type="text"/>	Date <input style="width: 10%;" type="text"/>	Signature <input style="width: 90%;" type="text"/>	
Information Owner (Internal Use Only)			
Name (Last, First, MI) <input style="width: 90%;" type="text"/>	Date <input style="width: 10%;" type="text"/>	Signature <input style="width: 90%;" type="text"/>	
Processor (Internal Use Only)			
Name (Last, First, MI) <input style="width: 90%;" type="text"/>	Date <input style="width: 10%;" type="text"/>	Signature <input style="width: 90%;" type="text"/>	
Privacy Act Statement			
Authority Purpose:	Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.		
Routine Uses:	To record names, signatures, and other identifiers for the purpose of validating individuals requesting access to Marine Corps Enterprise tools and information. NOTE: Records may be maintained in both electronic and/or paper form.		
Disclosure:	Disclosure of this information is voluntary; however, failure to provide the requested information may impede or prevent further processing of this request.		
<small>2015 Enterprise-ITSM AR Form v1.2.90</small>			

Appointment/Relief Letters and Endorsements



UNITED STATES MARINE CORPS
Unit Header

IN REPLY REFER TO:
5270
(Code)
(DATE)

From: (OIC Title, Unit)
To: (Rank FN MI, LN)
Via: (Section Head)

Subj: APPOINTMENT AS AN INFORMATION SYSTEMS COORDINATOR

Ref: (a) Force Order 5270.1

1. Per reference (a) you are hereby appointed as an Information Systems Coordinator (ISC) for (Section). You are to read and become familiar with the reference.

2. This appointment will remain in effect until you are relieved in writing by the appointing authority or transferred from this command.

(OIC SIGNATURE NAME)

FIRST ENDORSEMENT

From: (Rank FN MI, LN)
To: (OIC Title, Unit)
Via: (Section Head)

Subj: APPOINTMENT AS AN INFORMATION SYSTEMS COORDINATOR

1. I have read and understand the reference. I accept the appointment of the additional duty as an ISC.

(ISC SIGNATURE NAME)

Copy to:
MARFORRES G-6 RSD
MSC G-6

UNITED STATES MARINE CORPS
Unit Header



IN REPLY REFER TO:
5270
(Code)
(DATE)

From: (OIC Title, Unit)
To: (Rank FN MI, LN)
Via: (Section Head)

Subj: RELIEF AS AN INFORMATION SYSTEMS COORDINATOR

Ref: (a) Force Order 5270.1

1. Per reference (a) you are hereby relieved as an Information Systems Coordinator (ISC) for (Section).

2. Your appointment and relief letters will be maintained at Marine Forces Reserve G-6.

(OIC SIGNATURE NAME)

FIRST ENDORSEMENT

From: (Rank FN MI, LN)
To: (OIC Title, Unit)
Via: (Section Head)

Subj: RELIEF AS AN INFORMATION SYSTEMS COORDINATOR

1. I stand relieved as an ISC.

(ISC SIGNATURE NAME)

Copy to:
MARFORRES G-6 RSD
MSC G-6

Turnover Folder & Desktop Procedure Requirements

The continual rotation of Information System Coordinator (ISC) personnel results in competency and continuity gaps. ISC establishment and use of a turnover folder with desktop procedures will alleviate this deficiency (REF. MCO P4790.2c w/ch 1-2 17 DEC 12). The following documents will be included in the turnover folder/desktop procedures in addition to those items listed in the reference.

Turnover Folder. A turnover folder is a file containing pertinent information about a billet. When updated, maintained, and passed on it provides the basic information so that the recipient can assume duties in a minimum amount of time. The contents of a turnover folder shall include the following:

1. Letter of assignment for the current ISC.
2. Letter of relief for the previous ISC.
3. Unit Organizational chart.
4. ISC Chain of Command/Coordination.
5. A copy of Force Order 5270.1 as one of the pertinent references.

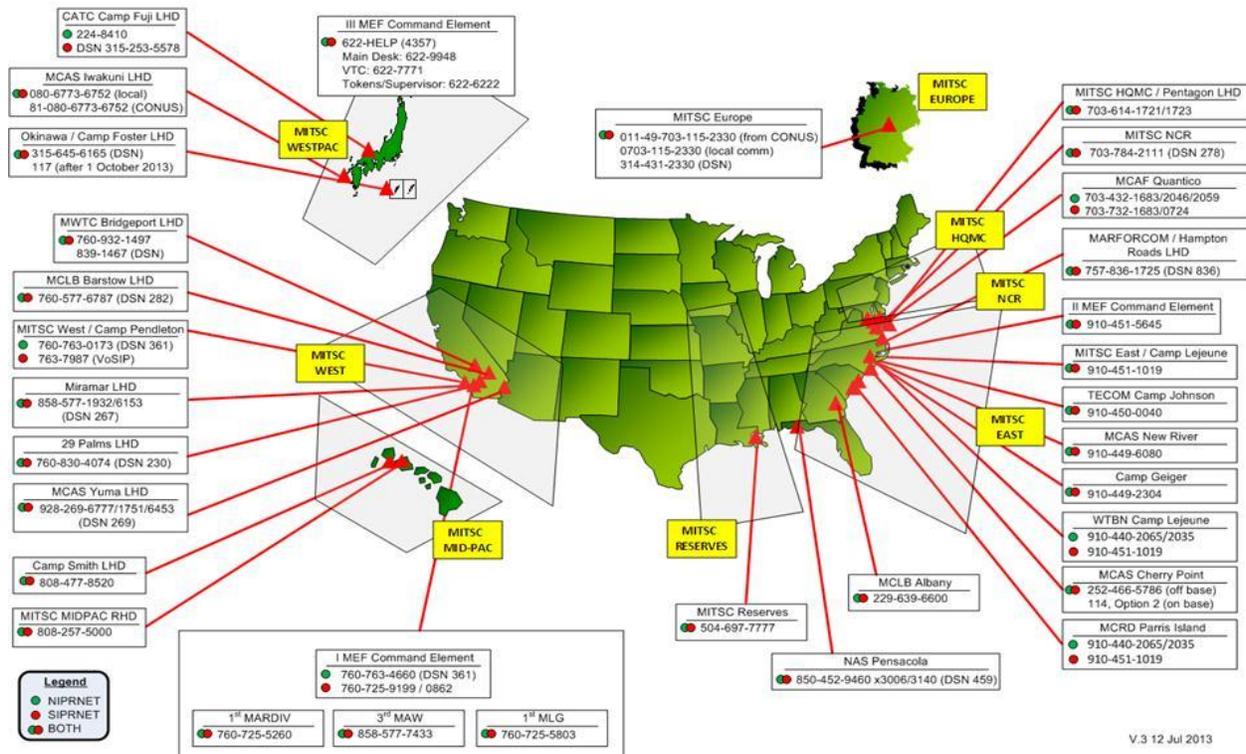
Desktop Procedures. Desktop procedures are the processes concerning the management of a billet terms of who, what, when, where, why, and how. These written procedures define the routine functioning of a billet. Desktop procedures are to include the following:

1. A list or matrix of the daily routine.
2. Charts reflecting the routine flow of work.
3. Work priorities within the section or office.

USMC Regional Service Desk Contact Information

Regional Service Desk	PHONE	DSN/OTHER	RSD Email
MITSC HQMC	703-614-1721	703-614-1723 (Pentagon LSD)	mitschqmc servicedesk@usmc.mil
MITSC NCR	703-784-2111	278-2111 (DNS)	mitscnrc servicedesk@usmc.mil
MITSC EAST	910-451-1019		mitsceast servicedesk@usmc.mil
MITSC RESERVES	504-697-7777		mitscreservesservicedesk@usmc.mil
MITSC MID-PAC	315- 457-5000	315-457-5000	mitscmidpacservicedesk@usmc.mil
MITSC WEST	760-763-0173	763-7987 (VoSIP) SIPR 361-1073 (DSN)	mitscwestservicedesk@usmc.mil
MITSC WESTPAC	011-81-611-745-6872 080-6773-6752 (local) (after OCT 1)	315-645-6872 (DSN) 81-080-6773-6752 (CONUS) (OCT 1)	mitscwestpacservicedesk@usmc.mil
MITSC EUR	011-49-703-115-2330 (from CONUS) 0703-115-2330 (local)	314-431-2330 (DSN)	mitsceuropeservicedesk@usmc.mil

MCEN Regional and Local Help Desks



V.3 12 Jul 2013