USMC GCCS-J ACCESS REQUEST

SUBMIT REQUEST TO:	RESPONSIBLE COMMANDS:	CONTACT NUMBER:
HQMC FM PLN SENIOR PLANNER	NCR, SCHOOL HOUSE	DSN: 255-1388 COMM: 703-695-1388
MARFORCOM JOPES/JCRM FM FORCE DEPLOYMENT OFFICER	MFR, II MEF, LOGCOM	DSN: 836-1636 COMM: 757-836-1636

Upon receipt of a GCCS account, users are responsible for the following:

1. Change your password upon initial logon to GCCS.
2. Do not allow anyone to use your personal user identification and password. Notify your FM if you suspect that your password has been compromised. Do not attempt to gain access to any system or network you have not specifically been authorized to use.
3. Do not leave your computer terminal unattended while logged into the GCCS network. Your workstation must have the mandatory GCCS screen saver software with password protection invoked and set in order to leave your workstation logged in during the workday as long as there are no uncleared personnel in your area. At the end of the workday, log out of the network and secure any removable media in accordance with current security procedures, unless area has been approved for the open-storage of Secret material.
4. Do not use Automated Information System (AIS) network hardware, software, device or service for non-official business.
5. All magnetic media used with a GCCS workstation must be marked with the appropriate classification label.
6. All application software not authorized, which includes bulletin board software, freeware, shareware and privately/personally procured software, is expressly prohibited from use on any GCCS computer system.
7. Classified information must be destroyed only by authorized means and by personnel cleared to the level of material being destroyed. Removable magnetic media (tapes or diskettes) shall be degaussed, removed from container and cut into strips of varying lengths before disposal. Printer ribbons shall be removed from container, cut into strips of varying lengths and placed into burn bags. Laser printer cartridges must be declassified. See Knowledge Today (KT) for procedures for specific printers. Contact the IS Security Office for guidance in destruction of other media (hard disks, removable disks, etc.).
8. Report any violations or suspected violations of security to the Directorate Information Systems Security Officer (ISSO) immediately.

USMC GCCS-J ACCESS REQUEST

Current Date	Rank/CIV/CTR	Last Name	First Name	M.I.

MOS	Billet	Command	Branch of Service	DSN Phone #

Bldg	Rm #	Rotation Date	Priority	Type of Request	Office Code

NIPRNET E-Mail	SIPRNET E-Mail

JOPES Strategic Server	Type of Account	GCCS-J UserID

Request Access

JOPES	SUB FM			JCRM	JCRM MODULES

JUSTIFICATION FOR REQUESTED ACCOUNTS	

DB Roles (Check all that apply)

JOPES SMS USER	☐	WEBSM ORGANIC	☐	WEBSM READ	☐	TRANSVIZ	☐
RQT	☐	JET	☐	TMT	☐		☐

*USERS REQUESTING TMT MUST COMPLETE THE LAST PAGE OF THIS FORM.

JOPES OPLAN Series Requested (Select all that Apply)

09	10-19	20-29	30-33	34-39

40-49	50-59	60-69	70-74	75-79

80-89	- Submit newsgroups* with a detailed list if access is required to restricted OPLAN's. - Submit newsgroups* for any permissions required above supporting component. * Server: GCCSDTA.MCW.AD.USMC.SMIL.MIL; Newsgroup: HQMC.0511COMMUNITY

I understand that access to GCCS is subject to monitoring and as a user I have no expectation of privacy with all user files. I further understand that misuse or unauthorized use of GCCS Information Systems can result in disciplinary action taken on behalf of the U.S. Government in accordance with the UCMJ and/or all applicable laws.

USMC GCCS-J ACCESS REQUEST

Requestor (After signed, save and email this document to your supervisor.)

Rank/CIV/CTR	Last Name	First Name	M.I.

Requestor's Digital Signature	

Requestor's Supervisor (After signed, save and email this document to security manager/ISSO.)

Rank/CIV/CTR	Last Name	First Name	M.I.

Supervisor's Digital Signature	

Requestor's Security Manager/ISSO (Once clearance information is filled out & signed, please save and return digitally signed document to requestor.)

Clearance Level	Clearance Date	Clearance Agency

Rank/CIV/CTR	Last Name	First Name	M.I.

Security/ISSO's Digital Signature	

Requestor: Your USMC GCCS-J Access Request form has been signed by your security manager. If you are at the school house or NCR, submit this form to PP&O, PLN Functional Manager (FM) for processing. All others submit form to your MARFOR/MEF Chief.

MARFOR/MEF Chief (After signed, save and email this document to MARFOR FM.)

Rank/CIV/CTR	Last Name	First Name	M.I.

MARFOR/MEF Chief Digital Signature	

MARFOR FM Approval

Rank/CIV/CTR	Last Name	First Name	M.I.

MARFOR FM Digital Signature	
☐ Approve for Sub-FM Permissions	

JOPES USER REQUEST FORM
ACCESS FOR TPFDD MANAGEMENT TOOL (TMT)

1. TMT is required to upload from feeder systems or download from JOPES database.
2. Access to TMT should be restricted to as few individuals as operationally feasible.
3. Access to TMT will only allow users read permissions to the 1000 series.
4. Failure to upload data into a working PID will terminate access to TMT immediately.
5. By digitally signing below, I acknowledge that the requesting individual understands how to properly operate TMT and will upload records only into working TPFDDs.

MSC Chief (After signed, save and email this document to the MARFOR/MEF Chief)

Rank/CIV/CTR	Last Name	First Name	M.I.

MSC Chief's Digital Signature	

MARFOR/MEF Chief (After signed, save and email this document to the MARFOR FM.)

Rank/CIV/CTR	Last Name	First Name	M.I.

MARFOR/MEF Chief Digital Signature	

MARFOR FM Approval

Rank/CIV/CTR	Last Name	First Name	M.I.

MARFOR FM's Digital Signature	