



UNITED STATES MARINE CORPS

MARINE FORCES RESERVE
MARINE FORCES NORTH
2000 OPELOUSAS AVENUE
NEW ORLEANS, LA 70146-5400

ForO 5239.2

G-6

19 Sep 2012

FORCE ORDER 5239.2

From: Commander

To: Distribution List

Subj: CYBER SECURITY WORKFORCE IMPROVEMENT PROGRAM (CSWIP)

Ref: (a) DoD 8570.01-M, "Information Assurance Workforce Improvement Program", May 15, 2008

(b) Force Policy Letter 06-11

(c) CMC White Letter No. 1-11

(d) MARADMIN 722/10

Encl: (1) Sample Cyber Security Workforce Assignment Letter

(2) Privileged-Level Access Agreement Acceptable Use Policy (AUP)

(3) Sample Cyber Security Workforce (CSWF) Revocation of Privilege Access Letter

1. Situation. Cyberspace and Cyber Security (CS) capabilities enable information sharing across all warfighting domains and are essential to achieving mission success. Our adversaries are acutely aware of this fact and continue to place heavy focus on developing aggressive cyber forces intent on exploiting vulnerabilities within our Command, Control, Communications, and Computers (C4) systems and networks. Employing technical controls alone (e.g. firewalls, intrusion detection systems, etc) is not enough to protect against cyber attacks. Growing a certified, professional CS and privileged user workforce that integrates learned security practices into their day-to-day duties is critical to protecting our networks, systems, and information, and sustaining our ability to provide the decision-makers with reliable information at the right time.

2. Mission. The mission of the CSWIP is to identify the CS Workforce (CSWF), delineate CS levels and associated training, and verify the CS workforce knowledge and skill level through standard certification testing. CS certification programs will produce a workforce with demonstrated abilities to perform the functions of their assigned positions. The CSWIP:

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

a. Identifies the CSWF by assigning personnel to appropriate CS levels in accordance with reference (a) and identifying the required training and certifications for those levels. This includes initial training for new CSWF members as well as refresher training for existing CSWF members.

b. Meets the CyberSecurity requirements specified in references (b) and (c).

c. Identifies the requirement to track CS personnel certifications and certification status.

d. Identifies the requirement to track military CS billets in manpower databases based on operational mission support and force structure requirements.

e. Establishes a baseline of validated (tested) knowledge that is relevant, recognized, and accepted across the Department of Defense (DoD).

f. Specifies the need to provide required training to DoD military and civilian employees.

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. The CSWF will provide security for Marine Forces Reserve (MARFORRES)/Marine Forces North (MARFORNORTH) and U.S. Marine Corps data and telecommunication networks, Information Technology (IT) infrastructure, applications and systems. CSWF functions focus on the development, accreditation, operation, management, and enforcement of security capabilities for networks and systems. All CSWF personnel are required to be qualified in their positions based on the category and level defined by reference (a). The purpose of this document is to outline how Workforce Improvement Program (WIP) certification requirements will be implemented within MARFORRES/MARFORNORTH.

(2) Concept of Operations. All members of the MARFORRES/MARFORNORTH IT community (Marines, civilians and contractors) who are identified as members of the CS workforce will submit a CSWF Assignment Letter, enclosure (1) to the MARFORRES Information Systems Security Manager (ISSM) and complete the appropriate training as identified in the CSWIP. The CS workforce includes but is not limited to (refer to Table 1 for further guidance):

(a) All personnel holding the 0689 MOS.

(b) All personnel appointed as Command Information Officers (CIO).

(c) All personnel appointed as Information Systems Security Managers (ISSM).

(d) All personnel appointed as Cyber Security Officers, including: Network Operations Personnel, Information System Security Officers, Unit Communications Security Managers, Certification Authority Representatives (CAR), and Information System Security Auditors.

(e) Personnel in the following categories, based on the assigned billet and the duties of that billet: MOS 02XX, MOS 06XX, MOS 28XX, system administrators, network officers and network and system administrators.

Table 1. MARFORRES Designated CSWF Positions

SECTION	POSITION TITLE / SYSTEM PRIVILEGES	PERMISSIONS	CERT LEVEL
All	System Administrators, DBA, APP Dev	Workstations, Servers, Infrastructure Devices	IAT II
	Program of Record (POR) Administrator	Applicable POR	
	Local Administrator	Workstation(s)	IAT I
	Application Administrator	Applicable Application	
Cyber	Certifying Authority Representative (CAR), Command Information Officer (CIO)	None	IAM III
	Information Systems Security Manager (ISSM)		
	Information Systems Security Officer (ISSO)	None	IAM I
	Helpdesk SNCOIC	Workstations, Servers, Network	IAT II
	Helpdesk Technician		
Video Teleconferencing (VTC) Coordinator / VOIP			

	Cyber Network Operations Officer, Cyber Networks Engineer	Tandberg, All VTC devices/technologies	IAT I
	OIC, MAGTF Network Operations Center (MITSC)	All	IAT III
	SNCOIC, MAGTF Network Operations Center (MITSC)		
	Comm/Data Chief, MAGTF Network Operations Center (MITSC)	None	IAM I
	IA Technician, MAGTF Network Operations Center (MITSC)	Workstations, Servers, Infrastructure Devices	IAT II
	EKMS Technician Administrator		
		All	IAT II
* EKMS *		All	IAT II

b. WIP certification requirements. Reference (a) mandates that within six months of assignment of CS duties, all military and Government civilian CSWF personnel must achieve the appropriate CS certification. Assignment letters will specify each CSWF member's required level of WIP certification based on applicable WIP category and level. During the six month grace period, all Cyber Security (CS) and privileged user duties will be closely supervised by WIP certified personnel designated at the same or higher CSWF level than those being supervised.

(1) Supervisors and leaders will ensure individuals obtain one of the required certifications for the appropriate certification level, as well as any necessary operating system or network environment qualifications.

(2) Certifications must remain active in accordance with the requirements of each certifying organization, which may include Continuing Professional Education (CPE) requirements that must be met in order to remain in the associated CSWF position.

(3) Personnel will not be issued elevated user privileges until they have returned an endorsed CSWF assignment letter and submitted a signed Privileged-Level Access Agreement, enclosure (2). All above required documents will be submitted to the MARFORRES ISSM.

(4) The Headquarters Marine Corps (HQMC) Command, Control, Communications, and Computers (C4) Cyber Branch is temporarily allowing designated military CSWF members to meet WIP Operating System qualification requirements through the completion of a MarineNet Computer Based Training (CBT) Operating System (O/S) security course that is most relative to the platform used most frequently by each given CSWF technician. However, MarineNet O/S course completion certificates will not meet WIP requirements indefinitely. IAT level I-III members will continue to aggressively pursue required commercial operating system qualification regardless of whether they have temporarily met the WIP O/S qualification requirement through completion of a relevant MarineNet CBT course.

(5) Table 2 identifies WIP certification requirements for CSWF at each proficiency level; additional IAT IA and Operating System (O/S) qualification mapping can be found at: https://www.cool.navy.mil/ia_documents/ia_ia_flow.htm

Table 2. IAT and IAM Levels I-III

CERT TYPE	IAT LEVEL I	IAT LEVEL II	IAT LEVEL III
IA	<ul style="list-style-type: none"> • A+ • Network+ • SSCP 	<ul style="list-style-type: none"> • GSEC • Security+ • SCNP • SSCP 	<ul style="list-style-type: none"> • CISA • GCIH • GSE • SCNA • CISSP (or Associate)
CERT TYPE	IAM LEVEL I	IAM LEVEL II	IAM LEVEL III
IA	<ul style="list-style-type: none"> • CAP • GISF • GSLC • Security+ 	<ul style="list-style-type: none"> • CAP • GSLC • CISM • CISSP 	<ul style="list-style-type: none"> • GSLC • CISM • CISSP (or Associate)
Operating System (O/S)	• Applicable O/S Qualification	• Applicable O/S Qualification	• Applicable O/S Qualification
Network Environment	• N/A	• CCNA	• CCNP

c. Waivers

(1) CS personnel must be fully trained and certified prior to deployment to a combat environment. A waiver for the period of the deployment can be approved for certified IAT-I's to fill level IAT-II or IAT-III billets (or for IAM-I's to fill level IAM-II or IAM-III billets) without attaining the appropriate certification while deployed to a combat environment. The interim waiver places an individual in a suspense status and must be time limited and include an expiration date not to exceed 6 months following date of return from combat status.

(2) Contractors are not eligible for CSWF certification waivers.

(3) Waivers will not extend beyond 6 months and must include an expiration date. Consecutive waivers for personnel are not authorized except as noted in reference (a). Waivers must be a management review item.

(4) Individuals requiring a waiver must contact the Cyber Security Section of MARFORRES.

d. WIP certification non-compliance. In accordance with reference (d), failure to meet WIP certification requirements at the expiration of the six month grace period will be cause for reassignment to a non-CSWF position, all privileged user access to be revoked, enclosure (3), and may result in termination of employment for civilian and contractor personnel.

e. WIP certification course options and exams. The Marine Corps will assume approved costs for initial CSWF certification courses, exams, and refresher training for CSWF members who have been assigned in writing. CSWF Marines must also be identified in authoritative Marine Corps training systems.

(1) MARFORRES Cyber Security Section. All requests for any level of Cyber Security training should be directed to the MARFORRES Cyber Security Manager (CSM) (MFR_G6_INFORMATION_ASSURANCE@usmc.mil). The Cyber Security Training Noncommissioned Officer is responsible for coordinating courses with the Communications Training Centers; Marine Corps Support Facility, New Orleans, Louisiana and will periodically host this training. Any persons seeking training should contact the MARFORRES Cyber Security Office.

(2) Other Sources. MarineNet and the Virtual Training Environment (VTE) both offer online CBT courses for several of the WIP required certification courses. VTE training can be found at: <https://www.vte.cert.org/vteweb/>

(3) In order to complete the certification, students must take an exam. The Marine Corps has funded a number of vouchers for these certification exams. Students that pass pre-exams at the end of the CSWF courses are then allowed to take the actual exam. If a student does not pass the pre-exam, additional time will be provided to prepare before a voucher is used for the certification exam.

f. Contractors. Contractors are responsible for providing the CSWF related training and exam costs for their personnel.

Unless otherwise stated in their contract/Statement of Work, contractors are not authorized to attend CTC courses. Contracting personnel are also not eligible to register for MarineNet CBT courses; however, they may request a VTE account through a DoD sponsor. Per reference (a), MARFORRES Contracting Officer's Technical Representatives (COTRs) are required to:

(1) Ensure that contracting positions requiring CS responsibilities to include privileged access by contractor personnel define certification requirements in the contract or statement of work in order to enforce WIP certification requirements.

(2) Ensure contracting personnel supporting CS (IAM, IAT, or IASE positions) are appropriately certified prior to being engaged.

(3) Ensure that contractor personnel are appropriately certified and provide verification to the MARFORRES ISSM.

(4) Support tracking contractors CS category, specialty, level, and certification qualification.

g. Tasks

(1) Contracting Officer's Technical Representatives (COTR). COTRs are to ensure full compliance with all requirements of this directive to avoid having contractors lose their privileged user access.

(2) Information Systems Security Manager (ISSM). The MARFORRES ISSM will ensure that all identified MARFORRES Headquarters (HQ) CSWF members (defined in Table 1) are assigned CSWF appointment letters. MARFORRES G-6 HQ personnel with privileged user access will sign an updated Privileged-Level Access Agreement, enclosure (2) and return the signed document to the MARFORRES CSM.

(3) MARFORRES G-6. MARFORRES G-6 will identify the names of all military, DoD civilian, and/or contractor personnel that currently have privileged access on any Marine Corps Enterprise Network (MCEN) system (to include Program of Record, applications, and/or network(s)). Individuals identified as having privileged user access will be assigned as a member of the command's CSWF and subject to all WIP certification requirements specified within this policy.

(4) MARFORRES/MARFORNORTH HQ Directorates and Staff, Major Subordinate Commands. Supervisors and Commanders will ensure that personnel identified as part of the CSWF are given sufficient time to prepare for and complete the required training within the identified waiver period.

4. Administration and Logistics. Direct all questions pertaining to this policy to the MARFORRES ISSM at 504-697-7697/7645/7620 or MARFORRES CS group mailbox (MARFORRESIA@usmc.mil).

5. Command and Signal

a. Command. This Order is applicable to the Marine Forces Reserve and Marine Forces North.

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



S. A. HUMMER

DISTRIBUTION: C, D

Directives issued by this Headquarters are published and distributed electronically. Electronic versions of the Force Directives can be found at:

<http://www.marines.mil/unit/marforres/MFRHQ/G1/Adjutant/G-1%20Adjutant%20Directives/default.aspx>



Sample Cyber Security Workforce Assignment Letter

UNITED STATES MARINE CORPS

MARINE FORCES RESERVE
MARINE FORCES NORTH
2000 OPELOUSAS AVENUE
NEW ORLEANS, LA 70146-5400

5239
G-6
(Date)

From: Information Systems Security Manager (ISSM)
To: Rank, Name, MOS/Position
Via: Include only when appointing personnel in another AC/S
Section

Subj: CYBER SECURITY WORKFORCE (CSWF) ASSIGNMENT LETTER

- Ref:
- (a) DoDI 8510.01, "Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)," Nov 28, 2007
 - (b) DoDD 8500.01E, Information Assurance IA) of 24 Oct 02, current as of Apr 23, 2007
 - (c) DoD 8570.01-M, "Information Assurance Workforce Improvement Program," May 15, 2008
 - (d) DoDI 8500.2, "Information Assurance (IA) Implementation," of Feb 6, 2003
 - (e) CJCSI 6510-01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," of 9 February 2011
 - (f) CJCSM 6510.01A, "Information Assurance (IA) and Computer Network Defense (CND) Volume 1 (Incident Handling Program)" of 24 June 2009
 - (g) MCO 5239.2A,
 - (h) USMC EIAD 010, "Unauthorized Disclosure and Electronic Spillage Handling", of Sep 2006
 - (i) SECNAVINST 5510.30B
 - (j) SECNAVINST 5510.36A
 - (k) ForO 5239.2

1. Your position, (position name), is a position of great responsibility and requires that you are certified as Information Assurance Technical (IAT), Level (I, II, III) member of the Cyber Security Workforce (CSWF) program in accordance with the references. After meeting all Cyber Security Workforce Improvement Program (CSWIP) requirements, you will be given unsupervised privileges on:

Enclosure (1)

Subj: CYBER SECURITY WORKFORCE (CSWF) ASSIGNMENT LETTER

- Workstations OS: Windows XP, 7
- Servers OS: Windows 2008 R2
- Applications:
- Network routing and switching systems
- N/A (IAM levels I-III and IASAE levels I-II)

2. IAT Level (I, II, II) Requirements:

a. Provide the Marine Forces Reserve (MARFORRES) Information Systems Security Manager (ISSM) with a copy of all required certifications.

b. Register certifications at:
<https://pki.dmdc.osd.mil/appj/dwc/>.

c. Develop a training and certification plan with your supervisor as soon as possible if you require additional certifications.

d. Maintain currency on Continuing Professional Education(CPE) requirements.

3. Your duties as the IAT include, but are not limited to:

a. Applying DoD regulations and policies to perform IA tasks, identify weaknesses, apply IA controls, and mitigate risks in accordance with references (a) through (k).

b. Receiving the necessary technical and IA training, education, and certification required to carry out respective duties. IATs duties and responsibilities are identified in references (c), (f) and (g).

c. Satisfying all responsibilities of an Authorized User as outlined in reference (c) and (g).

d. Ensuring that procedures are developed and implemented in accordance with configuration management policies and practices for authorizing the use of software on information systems.

e. Ensuring audit trails (system logs) are reviewed periodically, and that audit records are archived and maintained for future reference.

f. Coordinating security measures including analysis, periodic testing, evaluation, verification, accreditation, and review of information system installation at the appropriate

Subj: CYBER SECURITY WORKFORCE (CSWF) ASSIGNMENT LETTER

classification level within the command or organizational network structure.

g. Ensuring that compliance monitoring occurs by reviewing the results of such monitoring and notifying MARFORRES G6 Watch Officers of significant IA CAT I and II findings through remediation, transfer responsibilities, and mitigation violations (i.e., CAT I findings).

h. Recognizing potential security violations and ensuring that security violations and incidents are properly reported to the MARFORRES G6 Watch Officer, the MARFORRES G6 Cyber Security Branch Head, and DoD reporting chain, as required. This also includes monitoring the implementation of security guidance and coordinating and directing actions appropriate to remedy security deficiencies, and following procedures set forth in accordance with reference (j). Electronic spillage of classified information is reported in accordance with procedures set forth in reference (g).

i. Providing security oversight for Marine Forces Reserve and subordinate commands. This includes coordinating Marine Forces Reserve security measures such as analysis, periodic testing, evaluation, verification, accreditation, and review of information system installations at appropriate classification levels.

j. Conducting reviews of the Online Compliance Reporting System to ensure Information Assurance Vulnerabilities Alerts, Technical, Computer Tasking Orders, and bulletins are reported in accordance with Information Assurance Vulnerability Management directives.

k. Installing and operating IT systems in a test configuration environment that does not alter the program code or compromise IA security controls.

l. Ensuring that information ownership responsibilities are established for each information system to include accountability, access approvals, and special handling requirements.

4. Network, system, and/or application privileged access prerequisites:

a. You are required to comply with the security requirements of reference (i) and hold a U.S. Government

Subj: CYBER SECURITY WORKFORCE (CSWF) ASSIGNMENT LETTER

security clearance commensurate with the level of information processed by the information system(s) for which you are responsible.

b. You must sign acknowledgement of this appointment letter, route through your supervisor signature, and submit to the MARFORRES ISSM.

c. You must provide the MARFORRES ISSM with a Privileged-Level Access Agreement (reference (k), enclosure (2)).

5. You have **six months** from the date of this letter to meet all CSWIP certification requirements. Failure to do so will result in all government network, system, and/or application privileged access being revoked, reassignment to a non-CSWF position until proof of required certification(s) is provided, and may result in termination of employment for civilian and contractor personnel.

6. Should you lose your certification (due to not maintaining your credentials) or fail to maintain a current security clearance commensurate with required level for network(s) accessed as verified in the Joint Personnel Adjudication System (JPAS), your elevated privileges and CSWF responsibilities will be revoked. Direct all questions related to this CSWF assignment letter to the MARFORRES ISSM at: 504.697.7697.

SIGNATURE

Acknowledgements:

a. Member signature: _____ Date: _____

b. Supervisor (OIC or SNCOIC):

Name: _____ Signature: _____ Date: _____

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

INFORMATION SYSTEMS SECURITY MANAGER: _____

ISSM 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: _____

Sample Cyber Security Workforce (CSWF) Revocation of Privilege
Access Letter



UNITED STATES MARINE CORPS

MARINE FORCES RESERVE
MARINE FORCES NORTH
2000 OPELOUSAS AVENUE
NEW ORLEANS, LA 70146-5400

IN REPLY REFER TO:
5239
G-6
(Date)

From: Information Systems Security Manager (ISSM)
To: (Rank and Full Name MOS/Position)

Subj: CYBER SECURITY WORKFORCE (CSWF) REVOCATION OF
PRIVILEGE ACCESS

Ref: (a) DoD 8570.01-M, "Information Assurance Workforce
Improvement Program", May 15, 2008
(b) ForO 5239.2
(c) Cyber Security Workforce (CSWF) Assignment Letter

1. Per the references and signature on the Cyber Security Workforce Assignment Letter, you were authorized 6 months from the date of the assignment letter, to meet all Cyber Security Workforce (CSWF) Workforce Improvement Program (WIP) certification requirements. During your time as the **(BILLET)**, as an Information Assurance **(TECHNICIAN or MANAGER, Level XXX)** you have failed to meet these requirements. As stated on your CSWF Assignment Letter, the below privileges will be immediately revoked until you can produce the necessary certification that is required to perform your current billet.

- [] Workstations: OS: _____
- [] Servers OS: _____.
- [] Applications: _____
- [] Network routing and switching systems
- [] N/A (IAM levels I-III and IASAE levels I-III)

2. Direct all questions related to this CSWF revocation letter to the ISSM Officer at (504)697-7697/7645.

SIGNATURE