



**DEPARTMENT OF THE AIR FORCE
AIR FORCE INSTITUTE FOR ENVIRONMENT, SAFETY AND
OCCUPATIONAL HEALTH RISK ANALYSIS (AFIERA)
BROOKS AIR FORCE BASE TEXAS (AFMC)**

MEMORANDUM FOR All Command Core Systems Administrators

29 Mar 00

FROM: AFIERA/RSEC

SUBJECT: Command Core System (CCS) Security Measures Requirements Update

1. As many of you know, the CCS is currently completing the Health Affairs Level-2 Certification and Accreditation process. To obtain this level of certification, several business practices must be followed. The purpose of this memo is to notify CCS System Administrators and users of key procedures that need to be implemented immediately. This letter is not intended to be all-inclusive for CCS security measures. It is however intended to highlight some key procedures that must be immediately implemented and followed. Specifics are provided below:

a. System Administrator responsibilities:

(1) When a user is assigned a user ID and password, the system administrator **must** set the password to expire immediately requiring the user to change their password the first time it is used. This also applies to an existing user who has requested that their password be reset.

(2) The directory where the CCS objects (the .fmx and .rep files) are stored must be restricted to read access only for all users. Only the CCS SA should have write/update capabilities on this directory. The SA needs to get with the person(s) responsible for the server(s) that house these objects and verify the rights to the directory.

(3) Prior to a user being issued a CCS user ID and password, the CCS SA must ensure that the person has read and signed the CCS Security Awareness and Training Plan. A draft copy of this document has been posted on the CCS web site www.commandcore.com. Once the document has been accepted and is finalized, it will be distributed to all CCS System Administrators.

(4) All reports that are printed from CCS need to be stamped with "For Official Use Only." Until the reports can be modified, the CCS SA is responsible to provide a stamp to the users that can be used to annotate each page of a printed report as "For Official Use Only."

b. User responsibilities:

(1) CCS security measures prohibit multiple log-ins. Users will not log into CCS at more than one computer at a time.

(2) Users need to activate their computer's screen saver program with password protection.

(3) CCS security procedures require users to change passwords every 90-days. Users will use different passwords when their password expires (every 90 days). Previous passwords will not be reused for a period of at least one calendar year.

(4) All printed reports much contain the words "For Official Use Only" on each page. Users must stamp each page of printed reports with "For Official Use Only".

2. Your immediate implementation of these procedures is a critical link in the CCS Certification and Accreditation process. If you have systems questions, please contact the CCS Help Desk at DSN 240-4150 or Commercial (210) 536-4150. For policy or program issues contact Capt Agapito Lambert or myself at DSN 240-4863/6682 respectively. Thanks for your support.

Craig B. Dezell

CRAIG B. DEZELL, Maj, USAF, BSC
Chief, Command Core Program Management Office