

**ANNEX H**

**INFORMATION SYSTEM SECURITY PLAN**  
**(ISSP)**

**INFORMATION SYSTEMS SECURITY PLAN  
(ISSP)**

**Developed By:  
U.S. Army Corps of Engineers (USACE) Finance Center**

**31 July 1998**

**INFORMATION SYSTEMS SECURITY PLAN  
(ISSP)**

**Table of Contents**

		<u>PAGE</u>
SECTION	1. Basic Systems Information And Identification	1
SECTION	2. Sensitivity, Protection Requirements, Security Mode, and Minimum Trusted Class	3
SECTION	3. Risk Analysis and Management Review	3
SECTION	4. Identification of Threats/Vulnerabilities	4
SECTION	5. Implementation of Controls and Countermeasures	4
SECTION	6. Certification	4
SECTION	7. Accreditation	4
SECTION	8. Attachments	5

**INFORMATION SYSTEM SECURITY PLAN (ISSP)  
FOR  
THE CORPS OF ENGINEERS ENTERPRISE MANAGEMENT  
INFORMATION SYSTEM  
(CEEMIS)**

**1. BASIC SYSTEMS INFORMATION AND IDENTIFICATION.**

a. Systems Identification/Title: CORPS OF ENGINEERS ENTERPRISE MANAGEMENT INFORMATION SYSTEM (CEEMIS). The system identifier number is ??? (the first number is the system category, the second is the requirements statement number).

b. System Category: CEEMIS will serve as the US Army Corps of Engineers upward reporting system.

c. Type of Accreditation: Generic.

d. Status: Developmental.

e. System Overview: The Corps of Engineers Enterprise Management Information System (CEEMIS) will serve as the Army Corps of Engineers upward reporting system. It also will allow system interfaces to electronically exchange data with existing and legacy government information systems thus supporting time and resource conservation.

f. System Environment and Special Considerations:

(1) Sensitivity Designation: Unclassified-Sensitive Two (US-2).

(2) Operational Factors Affecting Security: To access CEEMIS, user IDs must be obtained from the User ID Password System (UPASS) Administrator. Additionally, a password must be granted to "log in" CEEMIS.

To restrict unauthorized modification of cost-sensitive information and to help preserve the integrity of the data, the following internal system controls have been established:

- Each prospective user must have a valid USERID/PASSWORD which is obtained from the local terminal area security officer (TASO), Information Systems Security Officer (ISSO), or the UPASS Administrator
- Users must be approved by the activity responsible employee as a valid CEEMIS user after the user logs on CEEMIS and establishes the user ID information and requests access
- Users are restricted use of CEEMIS menu options other than option 2 to request access or option 1 to exit until approval by the responsible employee.

All users approved for access to CEEMIS will be given an access level depending on the level of information needed to access. This places the security on the data being reported to the individual(s) that have a “need to know”.

All users will be given one of the following levels of access:

- District Level (1) – A user granted district level access will have the capability of creating/updating, viewing, and generating report data for their responsible field operating activity (FOA). The district level team member will be required to maintain the points of contact table for their responsible reports. The CEEMIS POC for the field activity will be required to maintain the FOA table for their applicable FOA.
- Division Level (2) – A user granted division level access will have the capability of viewing and generating report data for the districts within their division. An operating division team member that will be creating/updating report data for their districts will need to be identified as a district level employee.
- Command Level (3) – A user granted command level access will have the capability of viewing and generating report data for the entire command. The USACE Finance Center (UFC) team members will be given the UFC indicator and thus will have the capability of creating/updating, viewing and generating report data for any activity within the command. The UFC team member will be required to maintain all system command tables such as appropriations, and FOA codes.
- Database Administrator Level (4) – A user granted database administrator (DBA) level will have the capability of performing any all functions within the system. The DBA will be the owner and manager of all tables within the system.

A user granted a level 3 or 4 will also be granted an additional indicator as to whether or not they are employed at the UFC or the Headquarters, U.S. Army Corps of Engineers (HQUSACE).

CEEMIS has been designed to allow team members to generate reports for a specific District (FOA), an entire Division, a Laboratory or the entire Command based on the permissions granted. Report levels are based on the “need to know” requirement.

CEEMIS has been designed to work via menu choices or using a smart code to go directly to the point on entry. Smart code use is much more efficient. The user will need to utilize the F4 list from the smart code field until familiar with the application.

(3) System Interfaces: CEEMIS interfaces with CEFMS and the Project and Resource Information System for Management (PRISM). External system interfaces include the Defense Finance and Accounting System (DFAS) which includes the Program Budget Accounting System (PBAS) and ELECTRA, and the Treasury’s Government On-line Accounting Link System (GOALS).

g. Information Contacts.

(1) Information Systems Security Officer (ISSO):

NAME: ?

(2) Program Manager

NAME: Thomas L. Brockman

(901) 874-8413

**2. SENSITIVITY, PROTECTION REQUIREMENTS, SECURITY MODE, AND MINIMUM TRUSTED CLASS.**

a. Sensitivity Designation: US-2.

b. Protection Requirements:

(1) Integrity - Primary

(2) Availability - Primary

c. Security Mode of Operation: System High Mode.

d. Minimum Trusted Class. IAW AR 380-19, Information Systems Security, and Department of Defense (DoD) 5200-28 STD, DoD Trusted System Evaluation Criteria, minimum trusted system class C2 for the Automated Information System (AIS) is met.

**3. RISK ANALYSIS AND MANAGEMENT REVIEW.**

a. A risk analysis will be performed to assess the vulnerabilities of the system.

b. Due to strict operating procedures and other security measures in place, all data are considered to be within an acceptable degree of risk. All economically feasible actions have been implemented to provide maximum protection for hardware, software, files, site-generated material and material storage.

c. If changes occur and create risks in the computer's area, the ISSO will decide whether to continue operations. The ISSO has the authority to terminate operations if there is an unacceptable security risk. The Information Systems Security Manager (ISSM) will be notified of such instances.

d. Any planned changes to the physical structure, relocation or additions to this AIS will be reported to the ISSO and the ISSM.

e. Personnel will be familiar with and comply with the Standard Operating Procedure (SOP). The strict access control policy (the areas monitored by the ISSO and/or TASOs) provides additional security of AIS and data.

**4. IDENTIFICATION OF THREATS/VULNERABILITIES. CEEMIS**

threats/vulnerabilities include those identified and the risks considered for the Corps of Engineers Automation Plan (CEAP) accreditation. Other threats/vulnerabilities will be identified in the risk analysis.

**5. IMPLEMENTATION OF CONTROLS AND COUNTERMEASURES.**

a. Security measures have been implemented. The SOP, Attachment A, is being written to address administrative controls and protection of information. A Continuity of Operations Plan (COOP) will be established in the event of an emergency. Physical, environmental, communications, personnel, software, hardware, procedural, TEMPEST, and document security have been addressed in this accreditation document.

b. Personnel Security: IAW AR 380-67 personnel security standards have been established for those individuals who require access to US2 information.

c. Communications Security: Classified information will not be processed on CEEMIS.

d. TEMPEST: A facility TEMPEST Assessment/Risk Analysis is not required.

e. Hardware and Software: C2 protection of CEEMIS is embodied in the hardware and software.

**6. CERTIFICATION:** CEEMIS is taking the necessary steps for certification. The system security will be tested during the Independent Operational Test (IOT). An independent evaluation will follow the IOT. Upon completion of the independent test and evaluation (IOT&E), the designated accreditation authority (DAA) will issue a security certification.

**7. ACCREDITATION:** The Corps of Engineers Automation Plan (CEAP-IA) has received accreditation for the hardware, system software, network and communications. CEEMIS accreditation will be provided after the certification process has been completed.

**8. ATTACHMENTS:**

- a. Attachment A, CEEMIS, Standing Operating Procedure (SOP). TBP in a later milestone.
- b. Information Systems Security Officer (ISSO) Appointment Order. TBP

Prepared by:

\_\_\_\_\_  
ISSO Signature  
???  
(202) 761-1962

Reviewed by:

\_\_\_\_\_  
Stanley Wrenn  
Director, USACE Finance Center  
(901) 874-8410

Reviewed by:

\_\_\_\_\_  
ISSM Signature  
???  
(202) 761-8723