

# USER ACCESS REQUEST AND RESPONSIBILITY STATEMENT

(FH Suppl 1 to AR 380-19)

## PRIVACY ACT

**AUTHORITY:** 10 U.S.C. 3013. **PURPOSE:** To control access, through password and user identification codes, to automatic equipment. **ROUTINE USE:** To identify data processing and communications customers authorized access to data systems. **DISCLOSURE:** Voluntary. Failure to provide information may result in denial of access to automation systems.

### PART I. ACTION REQUESTED (Filled in by ISSO).

- a. Type of action: New Account ( ) Delete ( ) Change ( ) Renewal ( ) Contractor ( )
- b. TSACS Login I.D. affected (if action is other than a new account): \_\_\_\_\_
- c. Access requested on the following system(s) (check all that apply): Exchange ( ) TSACS ( ) DAISM ( ) PRWEB ( )  
OROS ABC ( ) SIDPERS ( ) Telephone PIN: \_\_\_\_\_ SIPRNET: \_\_\_\_\_
- d. For DAISM, enter Module name: \_\_\_\_\_
- e. Other or special requirements: \_\_\_\_\_

### PART II. REQUESTOR INFORMATION (Filled in by user) except where noted, all entries are required for new accounts.

- a. Name (Last, First, MI): \_\_\_\_\_
- b. Title: \_\_\_\_\_ c. SSN: \_\_\_\_\_ d. Duty Telephone Number: \_\_\_\_\_
- e. Office Symbol: \_\_\_\_\_ f. Building/Room Number: \_\_\_\_\_ g. Organization: \_\_\_\_\_
- h. E-mail Address (required for TSACS accounts only): \_\_\_\_\_

### PART III. SECURITY ACCESS VERIFICATION (Filled in by Organizational Security Officer)

- a. Security Access Level: NAC or ENTNAC ( ) SECRET ( ) TS ( )
- b. Security Manager \_\_\_\_\_
- |                    |            |           |
|--------------------|------------|-----------|
| PRINTED/TYPED NAME | DUTY PHONE | SIGNATURE |
|--------------------|------------|-----------|

### PART IV. RESPONSIBILITIES REQUIREMENTS (Filled in by Requesting Organization and System Proponent).

As a potential user of Government information systems security resources, I am aware of the following responsibilities: I will use the resources only in the performance of my official duties. I will control and protect all data, software, hardware, passwords, copyrighted, or proprietary material to the best of my abilities. I will not use personally owned computers to access Government information systems security resources. I will immediately report suspected security incidents to my IASO. I will protect my user account name and password, and telephone access numbers at a level commensurate with the level of information being processed or accessed. I will abide by applicable security regulations and guidelines, and access only the resources authorized. I understand the password I receive as a result of this request is my personal access key and if I reveal my password to anyone, the password will be considered compromised and my access privilege suspended or revoked pending an investigation of the compromise.

- a. Requesting Individual: I have read the above and will comply to the best of my ability.

Printed Name	Duty Phone	Date	Signature
--------------	------------	------	-----------

- b. Supervisor: I verify this access request is authorized.

Printed Name	Duty Phone	Date	Signature
--------------	------------	------	-----------

- c. IASO: I verify user has proper security clearance, understands security guidelines, is an authorized user.

Printed Name	Duty Phone	Date	Signature
--------------	------------	------	-----------

- d. Contracting Officer Representative (COR)/Contract Monitor (CM): I certify this request and authorization is required under the scope of the existing contract Company Name: \_\_\_\_\_ Contract Number: \_\_\_\_\_

Contract/access expires on (provide date required entry): \_\_\_\_\_

Printed Name	Duty Phone	Date	Signature
--------------	------------	------	-----------