SYSTEM AUTHORIZATION ACCESS REQUEST (2875/SAAR)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
ROUTINE USES: None.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST
[X] INITIAL [ ] MODIFICATION [ ] DEACTIVATE USER ID _____

DATE *(YYYYMMDD)*

US BICES-X SYSTEM NAME *(Platform or Applications)* US BICES
If other, add network name here (DO NOT add BILAT/MULTILAT Names/Numbers)

LOCATION / SITE ID
Select Location From Menu

PART I *(To be completed by Requestor)*

1. NAME *(Last, First, Middle Initial)*	2. ORGANIZATION	
3. OFFICE SYMBOL/DEPARTMENT	4. PHONE *(DSN / Commercial / USBICES)*	
5. OFFICIAL E-MAIL ADDRESS, (e.g. @mail.mil)	6. GRADE/RANK (e.g. GS15/CIV or O4/MAJ or CTR)	
7. OFFICIAL MAILING ADDRESS	8. NATIONALITY / AFFILIATION [ ] US [X] FN 3 Letter Country Identifier	9. DESIGNATION OF PERSON [X] MILITARY [ ] CIVILIAN [ ] CONTRACTOR

10. CYBER AWARENESS TRAINING CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*
[ ] I have completed annual Cyber Awareness Certification Training DATE *(YYYYMMDD)* _____

11. USER SIGNATURE	12. DATE *(YYYYMMDD)*

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR*(If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)*

13. JUSTIFICATION FOR ACCESS Select Type of Access: Select One...

14. TYPE OF ACCESS REQUIRED:
[X] AUTHORIZED [ ] PRIVILEGED

15. USER REQUIRES ACCESS TO:
[ ] UNCLASSIFIED [X] CLASSIFIED *(Specify category)* Secret Releasable
[ ] OTHER _____

16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. [X]	16a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)*	
17. SUPERVISOR'S NAME *(Print Name)* LAST, FIRST, MI.	18. SUPERVISOR'S SIGNATURE	19. DATE *(YYYYMMDD)*
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT	20a. SUPERVISOR'S E-MAIL ADDRESS	20b. PHONE NUMBER
21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER	21b. DATE *(YYYYMMDD)*

22. SIGNATURE OF IAO OR APPOINTEE	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE *(YYYYMMDD)*

DD FORM 2875, AUG 2009 - US BICES (Updated), FEB 2022 Adobe Designer 9.0

26. NAME *(Last, First, Middle Initial)*

27. OPTIONAL INFORMATION *(Additional information)*

TNE User Category

-- Signed Acceptable Use Policy (AUP): ☒ YES ☐ NO

☐ **1 - Read/Write/Re-label** (e.g. FDOs, managers)

☐ **2 - Read/Write** (e.g. analysts)

☐ **3 - Read only** (e.g. data consumers)

Network TNE is accessed from:

If the network is sensitive, this form must be protected as appropriate.

****

Unit Security Manager or SSO must complete and sign part III verifying security clearance level of user and validating current NATO Read On in Block 28b (when applicable).

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION *(YYYYMMDD)*	
28b. CLEARANCE LEVEL Clearance + NATO Read On for US BICES		28c. IT LEVEL DESIGNATION ☒ LEVEL I ☐ LEVEL II ☐ LEVEL III	
29. VERIFIED BY *(Print name)*	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE *(YYYYMMDD)*

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED *(YYYYMMDD)*	PROCESSED BY *(Print name and sign)*	DATE *(YYYYMMDD)*
DATE REVALIDATED *(YYYYMMDD)*	REVALIDATED BY *(Print name and sign)*	DATE *(YYYYMMDD)*

INSTRUCTIONS

The prescribing document is as issued by using DoD Component.

A. PART I: The following information is provided by the user when establishing their USER ID.

(1) Name. The last name, first name, and middle initial of the user.

(2) Organization. The user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).

(3) Office Symbol/Department. The office symbol within the current organization (i.e. SDI).

(4) Telephone Number/DSN. The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial or US BICES phone number.

(5) Official E-mail Address. Email address where account credentials will be sent (must be .mil, bices.org, nato.int, .gov - not company or personal email)

(6) Job Title/Grade/Rank. The user's job title (Example: Systems Analyst, GS-14; Pay Clerk, GS-5) or military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.

(7) Official Mailing Address. The user's official mailing address.

(8) Citizenship (US, Foreign National, or Other). If Foreign National, please write/type User's 3 letter nation identifier code in next field.

(9) Designation of Person (Military, Civilian, Contractor)

(10) Cyber Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual DoD Approved Cyber Awareness Certification Training and the date.

(11) User's Signature. User must sign the DD Form 2875 with the understanding that they are responsible and accountable for their password and access to the system(s).

(12) Date. The date that the user signs the form.

B. PART II: The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

(13). Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.

(14) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters, or settings.)

(15) User Requires Access To: Place an "X" in the appropriate box. Specify category.

(16) Verification of Need to Know. To verify that the user requires access as requested.

(16a) Expiration Date for Access. The user must specify expiration date.

(17)) Supervisor's Name. The supervisor or command sponsor prints his/her name to indicate that the above information has been verified and that access is required.

(18) Supervisor's Signature. Supervisor's or command sponsor's signature is required by the endorser or his/her representative.

(19) Date. Date supervisor signs the form.

(20) Supervisor's organization and department.

(20a) E-mail Address. Supervisor's or command sponsor's email address.

(20b) Phone Number. Supervisor's or command sponsor's telephone number.

(21)) Signature of Information Owner/OPR. (Authorized signer varies based on Network ownership.)

(21a) Phone Number.

(21b) Date.

(22) Signature of local TASO, Regional ISSO, or enclave AO.

(23) Organization/Department of Local TASO, ISSO, or AO.

(24) Phone Number of Local TASO, ISSO, or AO.

(25) Date the local TASO, ISSO, or AO signs the Form.

(26) Name - Last name, first name, and middle initial of the user.

(27) Optional Information. (This item is intended to add additional information, as required.)

C. PART III: Certification of Background Investigation or Clearance.

(28) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).

(28a) Date of Investigation. Date of last investigation.

(28b) Clearance Level. The user's current security clearance level (i.e., Secret). For US BICES users, also include user's current NATO Read on level (e.g. NATO Secret)

(28c) IT Level Designation. The user's IT designation (Level I, Level II, or Level III).

(29) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.

(30) Phone number of the Security Manager or his/her representative.

(31) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.

(32) Date. The date that the form was signed by the Security Manager or his/her representative.

D. PART IV: This information is site specific and can be customized by either the DoD, functional activity, or the customer with approval of the DoD. This information will specifically identify the access required by the user.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

FILING: Original 2875/SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO. Recommend file be maintained by IAO adding the user to the system.

DD FORM 2875 INSTRUCTIONS, AUG 2009 - US BICES (Updated), FEB 2022