System Authorization Access Request (DD FORM 2875, AUG 2009) SAMIS/AFSAC Online/Report2Web (FeTODS/ETOs/ITOs)

These step-by-step instructions are intended to help you acquire access to the AFSAC managed information systems. Users requesting or modifying an AFSAC Online (AOL) account must also possess a Security Cooperation Information Portal (SCIP) account.

- To acquire a SCIP account, please go to: https://www.scportal.us/SCIPRegistration/introduction.jsp
  - How to register for access to AOL through the SCIP form:
    - When prompted for user role, select no role.
    - When prompted for communities to which you need access, select USAF Community.
    - When on the community target page, check the box for AFSAC Online.
  - For assistance with the SCIP registration process, please contact the SCIP Help Desk at dsca.sciphelp@mail.mil.

Note:

AFSAC REQUIRES FORMS TO BE ELECTRONICALLY COMPLETED TO ENSURE ACCURACY AND TIMELINESS FOR OBTAINING YOUR ACCOUNT.

SUBMITTED FORMS NOT PROPERLY COMPLETED WILL BE RETURNED.

ONLY THE TEMPLATES LOCATED ON THE AFSAC ONLINE HOMEPAGE (https://afsac.wpafb.af.mil/register.jsp) OR ON OUR DD 2875 PROCESSING SITE (https://cs2.eis.af.mil/sites/21268/ASAR/system/index.aspx#!/forms) WILL BE ACCEPTED. ALL OTHER DD 2875s WILL BE RETURNED.

Return to the Registration webpage (browser back arrow) or https://afsac.wpafb.af.mil/register.jsp

- Click on the appropriate form hyperlink for the system to which you are applying.
- Before making any changes, download the form and save to your computer.
- Open the form in ADOBE and enable all features.
- All required blocks must be completed before the request will be processed.

To complete the form, follow the steps below:

TYPE OF REQUEST:

- Initial: New user accounts and accounts that need to be re-established due to deletion.
- Modification: Changes to an existing account.
- Deactivate: Delete the user account.
- User ID: This is no longer required.

DATE: Enter the date of the request. (All dates must be entered in YYYYMMDD format.) NOTE: DD2875 must be dated within 30 days of submission date. Submitted forms dated over 30 days from day of submission will be rejected.

SYSTEM NAME: This block will be pre-populated. Ensure the system name matches the system you are requesting. If the system does not match the system you are requesting, download the correct template from the link above.

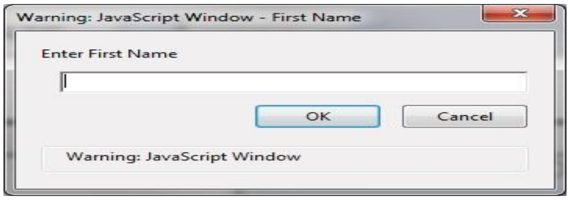
System Authorization Access Request (DD FORM 2875, AUG 2009) SAMIS/AFSAC Online/Report2Web (FeTODS/ETOs/ITOs)

Note: Report2Web - Users requiring access to FeTODS/ETOs/ITOs information must submit a separate Report2Web (FeTODS/ETOs/ITOs) DD 2875 account request for access to those systems. ***ATTENTION* Only SATODS and certain AFSAC personnel are permitted Report2Web (FeTODS/ETOs/ITOs) accounts. Standard USG users do not require these accounts and should not submit these types of requests.** For training purposes, a complete Report2Web tutorial is available through the AFSAC Online homepage.

LOCATION: Pre-populated. Do not change.

PART I and PART II (*Blocks to be completed by Requestor*):

1. **Name**: Enter full name in the pop-up windows. Three pop-up windows will appear for Last Name, First Name, and Middle Initial.



Warning: JavaScript Window - First Name

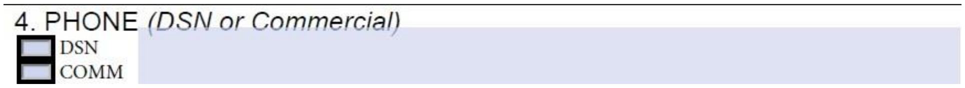
Enter First Name

Warning: JavaScript Window

2. **Organization**: Enter full unit name. (e. g., Air Force Life Cycle Management Center)

3. **Office Symbol/Department**: Enter unit office symbol or department name. (e. g., WFSZ)

4. **User's Phone Number**: Check DSN (Defense Switched Network) or Commercial and then enter the appropriate number including area code for commercial numbers.



4. PHONE *(DSN or Commercial)*

□ DSN
□ COMM

5. **User's Official Email Address**: Enter official e-mail address.

6. **Job Title & Grade/Rank**: Enter job title and grade/rank.
   - Contractors enter "CTR" as the grade/rank.

7. **Official Mailing Address**: Enter official mailing address.

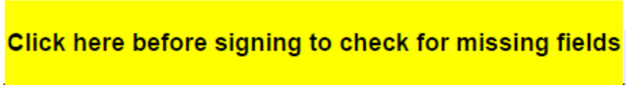
8. **Citizenship**: Select US or FN (Foreign National) or OTHER as appropriate.

9. **Designation of Person**: Select MILITARY, CIVILIAN or CONTRACTOR.

10. **IA Training and Awareness Certification Requirements**: Check the – "I have completed Annual Information Awareness Training." block and *enter the Date of Training in the stated format*. Check ADLS to obtain training date. (** **The IA date can be no more than one year prior to the date of submission.** **) Click here to access ADLS.

11. **User Signature:** Prior to signing the form, the user must ensure that blocks 1-13b or 1-16a are appropriately completed. The user may click the yellow box before signing to check for missing

fields. Once all required fields are completed, the yellow box will go away and the user may sign. **Only a digital signature is acceptable.**

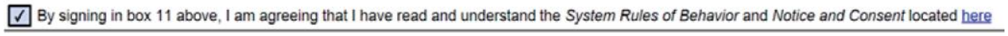


Click here before signing to check for missing fields

12. **Date:** Enter date in YYYYMMDD format.
13. **Justification for Access:** Provide the PURPOSE of the system access required and the access being requested. This **CANNOT** be a generic statement, such as "Access required to perform job duties".

    Example of a valid justification: *As a line manager on an LOA I need to be able to input data on new contract and update as necessary. I also review status for what is on order to see where I can be of assistance for another International Partner.*

System Rules of Behavior and Notice and Consent Checkbox: Read and acknowledge understanding of the System Rules of Behavior and Notice and Consent agreement. This can be found by clicking the hyperlink in block 13 on the form (see diagram below).



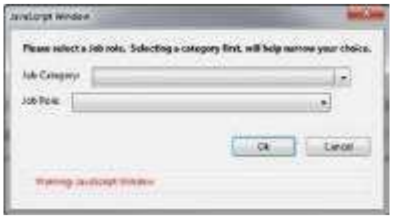
☑ By signing in box 11 above, I am agreeing that I have read and understand the *System Rules of Behavior* and *Notice and Consent* located here

13a. **Job Role:** Clicking the area beside the JOB ROLE will bring up the pop-up window below. Note: If you have an AFSAC Online or SAMIS account already the job roles must match.

Job Category: Select job category from the dropdown.
Job Role: Select the job role you perform using the dropdown.

Click HERE for SAMIS Job Role Matrix (Right click and select "Copy link location")

Click HERE for AOL Job Role Matrix (Right click and select "Copy link location")



JavaScript Window

Please select a Job role. Selecting a category first will help narrow your choice.

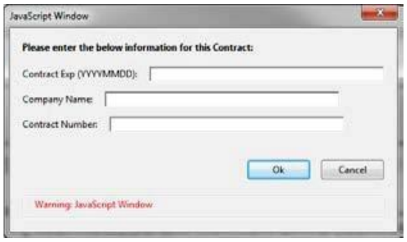
Job Category:

Job Role:

13b. **PIN:** Enter a four-digit numeric PIN that is easily remembered. The PIN is used for the creation of the initial password and thereafter when requesting password resets.

16a. **Access Expiration Date (Contractors only):** Enter the date that access is to be terminated. Contractors must specify company name, contract number, and expiration date. Use block 27 if additional space is required. Contractor accounts expire on the contract expiration date. An updated DD 2875 is required to prior to the current contract expiration date in order to keep the account active. Clicking in block 16a will bring up the pop-up window below.

System Authorization Access Request (DD FORM 2875, AUG 2009)
SAMIS/AFSAC Online/Report2Web (FeTODS/ETOs/ITOs)



Please enter the below information for this Contract:

Contract Exp (YYYYMMDD):

Company Name:

Contract Number:

*****User Portion is now complete*****

***** Ensure you have signed the form in block 11 *****

Please save the form using the naming convention below and send to your supervisor for further processing. [System] – [Last], [First] – DD-2875.pdf (e.g. SAMIS – Doe, John – DD-2875.pdf)

PART II (*Blocks to be completed by Supervisor*):

13. **Justification for Access:** Verify the requestor's justification. This is the **PURPOSE** of the system access required and the access being requested. This entry **CANNOT** be a generic statement, such as "Access required to perform job duties."

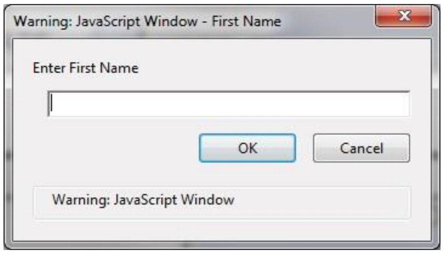
    Example of a valid justification: *As a line manager on an LOA I need to be able to input data on new contract and update as necessary. I also review status for what is on order to see where I can be of assistance for another International Partner.*

14. **Type of Access Required:** Item pre-selected according to job role.

15. **User Requires Access to:** Item pre-selected – "Unclassified"

16. **Verification of Need to Know**: This block should be checked, acknowledging supervisor's verification that the requestor has a valid need for access to the system.

17. **Supervisor's Name:** Enter Supervisor name. Enter full name in the pop-up windows. Three pop-up windows will appear for Last Name, First Name, and Middle Initial.


Warning: JavaScript Window - First Name
OK
Cancel
Warning: JavaScript Window

Enter First Name

18. **Supervisor's Signature:** Must be a digital signature. Error will remain until the blocks are filled out. Click the yellow box to check for missing fields before signing:

Supervisor click here before signing

System Authorization Access Request (DD FORM 2875, AUG 2009) SAMIS/AFSAC Online/Report2Web (FeTODS/ETOs/ITOs)

19. **Date:** Enter the date the document was signed. Must match date of digital signature.

20. **Supervisor's Organization/Department:** Enter organization/department. 20a. **Supervisor's E-mail Address:** Enter e-mail address.

20b. **Phone Number:** Enter phone number.

*****Supervisor Portion Complete*****
***** Ensure you have signed in block 18 *****

Part III needs to be filled out by your Security Manager to complete the form. Please follow the relevant instructions below:

<u>AFSAC employees</u>: Please upload to https://cs2.eis.af.mil/sites/21268/ASAR/system/index.aspx#!/submit for processing. Note, you must use Internet Explorer to upload the form.

<u>Non-AFSAC employees</u>: Please forward form to your security manager for further processing. Your command **Security Manager** or **Personnel Security Specialist** should accomplish this section. Once the form has been completely filled out by your security

Upload to our DD 2875 processing tool located at https://cs2.eis.af.mil/sites/21268/ASAR/system/index.aspx#!/submit

USG personnel will need to email their FETODS form to AFLCMC.WFNB.Workflow@us.af.mil for approval.

All others (e.g., DFAS, Army, Navy, etc.): Email to AFLCMC.WFRQ.DD2875@us.af.mil

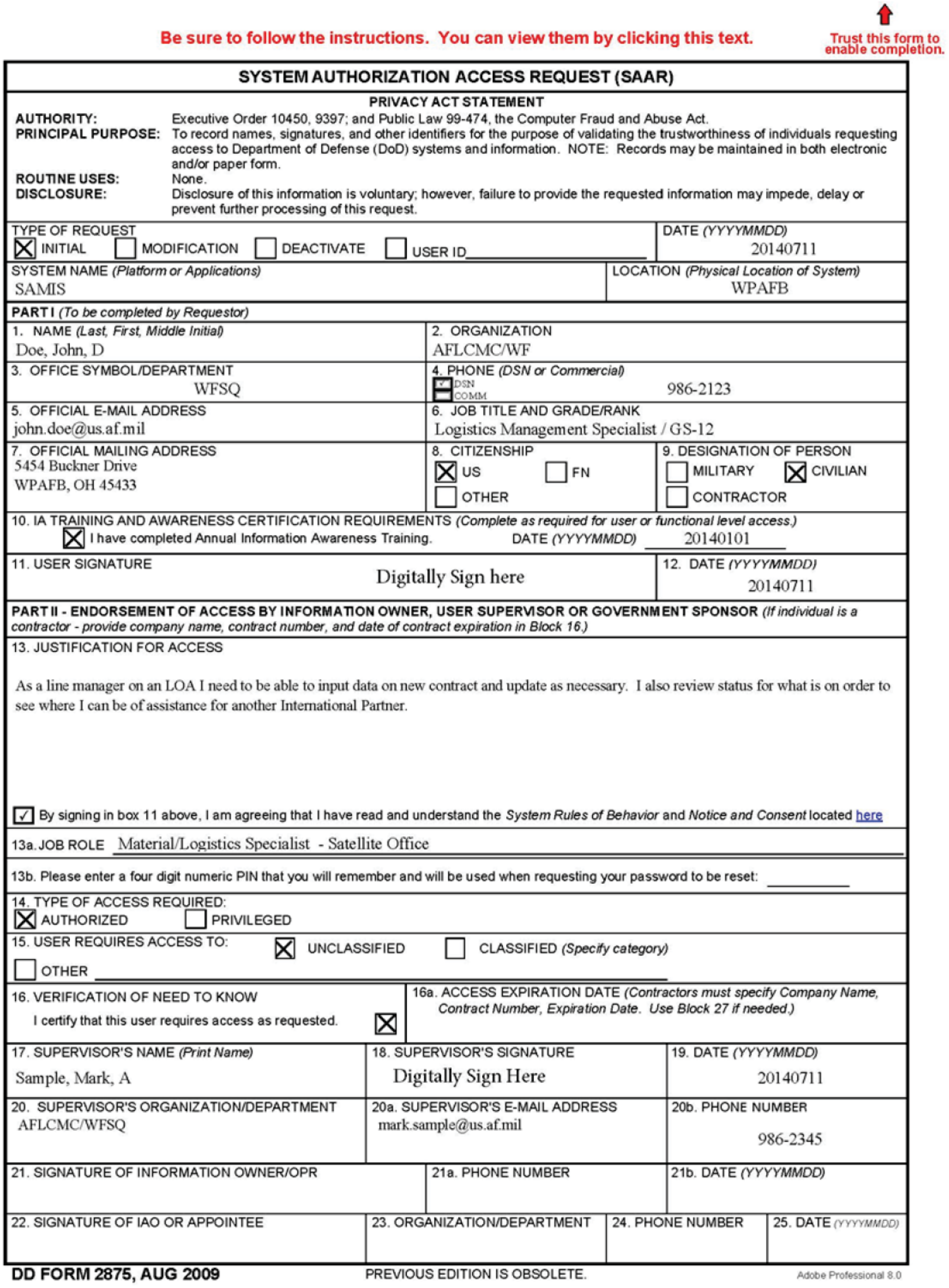
System Authorization Access Request (DD FORM 2875, AUG 2009) SAMIS/AFSAC Online/Report2Web (FeTODS/ETOs/ITOs)

ACRONYM LISTING:

Acronym	**Definition**
ADLS	Automated Distributed Learning System
AFSAC	Air Force Security Assistance Cooperation
AOL	AFSAC Online
CTR	Contractor
DSN	Defense Switch Network
ETO	Electronic Technical Order
FeTODS	Foreign Military Sales Electronic Technical Order Distribution System
FN	Foreign National
ITO	Interim Technical Order
LOA	Letter of Acceptance
PIN	Personal Identification Number
SAAR	System Authorization Access Request
SAMIS	Security Assistance Management Information System (AF)
SATODS	Security Assistance Technical Order Data System
SCIP	Security Cooperation Information Portal
TODO	Tech Order Distribution Office
USG	United States Government

System Authorization Access Request (DD FORM 2875, AUG 2009) SAMIS/AFSAC Online/Report2Web (FeTODS/ETOs/ITOs)

Example of Completed DD Form 2875:



Be sure to follow the instructions. You can view them by clicking this text.

Trust this form to enable completion.

SYSTEM AUTHORIZATION ACCESS REQUEST (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: ☒ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☐ USER ID ____________

DATE *(YYYYMMDD)*: 20140711

SYSTEM NAME *(Platform or Applications)*: SAMIS

LOCATION *(Physical Location of System)*: WPAFB

PART I *(To be completed by Requestor)*

1. NAME *(Last, First, Middle Initial)*: Doe, John, D

2. ORGANIZATION: AFLCMC/WF

3. OFFICE SYMBOL/DEPARTMENT: WFSQ

4. PHONE *(DSN or Commercial)*: ☑ DSN ☐ COMM 986-2123

5. OFFICIAL E-MAIL ADDRESS: john.doe@us.af.mil

6. JOB TITLE AND GRADE/RANK: Logistics Management Specialist / GS-12

7. OFFICIAL MAILING ADDRESS:
5454 Buckner Drive
WPAFB, OH 45433

8. CITIZENSHIP: ☒ US ☐ FN ☐ OTHER

9. DESIGNATION OF PERSON: ☐ MILITARY ☒ CIVILIAN ☐ CONTRACTOR

10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*
☒ I have completed Annual Information Awareness Training. DATE *(YYYYMMDD)* 20140101

11. USER SIGNATURE: Digitally Sign here

12. DATE *(YYYYMMDD)*: 20140711

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

As a line manager on an LOA I need to be able to input data on new contract and update as necessary. I also review status for what is on order to see where I can be of assistance for another International Partner.

☑ By signing in box 11 above, I am agreeing that I have read and understand the *System Rules of Behavior* and *Notice and Consent* located here

13a. JOB ROLE: Material/Logistics Specialist - Satellite Office

13b. Please enter a four digit numeric PIN that you will remember and will be used when requesting your password to be reset: __________

14. TYPE OF ACCESS REQUIRED: ☒ AUTHORIZED ☐ PRIVILEGED

15. USER REQUIRES ACCESS TO: ☒ UNCLASSIFIED ☐ CLASSIFIED *(Specify category)*
☐ OTHER ____________

16. VERIFICATION OF NEED TO KNOW
I certify that this user requires access as requested. ☒

16a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)*

17. SUPERVISOR'S NAME *(Print Name)*: Sample, Mark, A

18. SUPERVISOR'S SIGNATURE: Digitally Sign Here

19. DATE *(YYYYMMDD)*: 20140711

20. SUPERVISOR'S ORGANIZATION/DEPARTMENT: AFLCMC/WFSQ

20a. SUPERVISOR'S E-MAIL ADDRESS: mark.sample@us.af.mil

20b. PHONE NUMBER: 986-2345

21. SIGNATURE OF INFORMATION OWNER/OPR

21a. PHONE NUMBER

21b. DATE *(YYYYMMDD)*

22. SIGNATURE OF IAO OR APPOINTEE

23. ORGANIZATION/DEPARTMENT

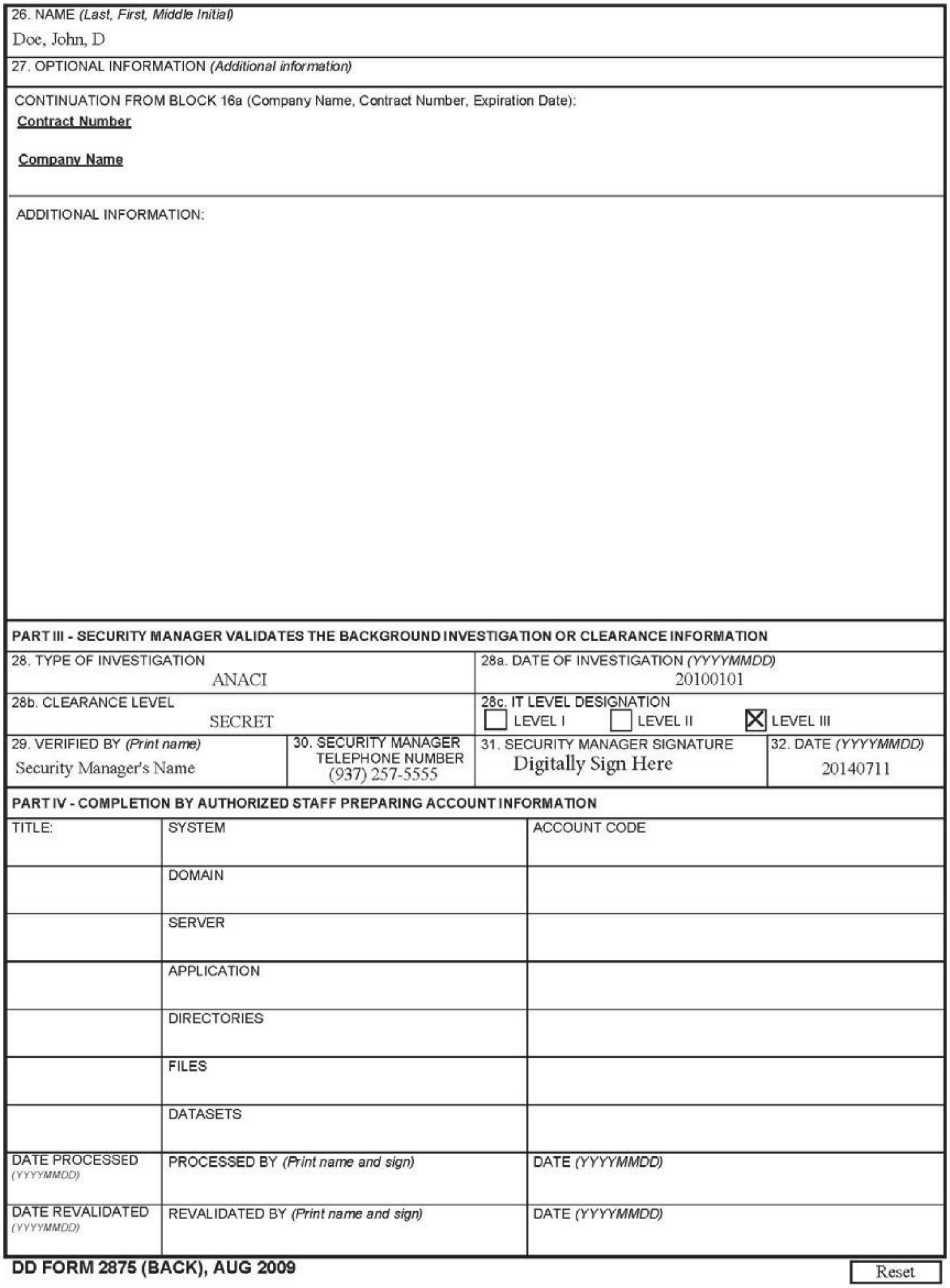
24. PHONE NUMBER

25. DATE *(YYYYMMDD)*

DD FORM 2875, AUG 2009 PREVIOUS EDITION IS OBSOLETE. Adobe Professional 8.0

System Authorization Access Request (DD FORM 2875, AUG 2009) SAMIS/AFSAC Online/Report.Web (FeTODS/ETOs/ITOs)

Example of Completed DD Form 2875 (continued):



26. NAME *(Last, First, Middle Initial)*
Doe, John, D

27. OPTIONAL INFORMATION *(Additional information)*

CONTINUATION FROM BLOCK 16a (Company Name, Contract Number, Expiration Date):

Contract Number

Company Name

ADDITIONAL INFORMATION:

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

28. TYPE OF INVESTIGATION
ANACI

28a. DATE OF INVESTIGATION *(YYYYMMDD)*
20100101

28b. CLEARANCE LEVEL
SECRET

28c. IT LEVEL DESIGNATION
☐ LEVEL I ☐ LEVEL II ☒ LEVEL III

29. VERIFIED BY *(Print name)*
Security Manager's Name

30. SECURITY MANAGER TELEPHONE NUMBER
(937) 257-5555

31. SECURITY MANAGER SIGNATURE
Digitally Sign Here

32. DATE *(YYYYMMDD)*
20140711

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

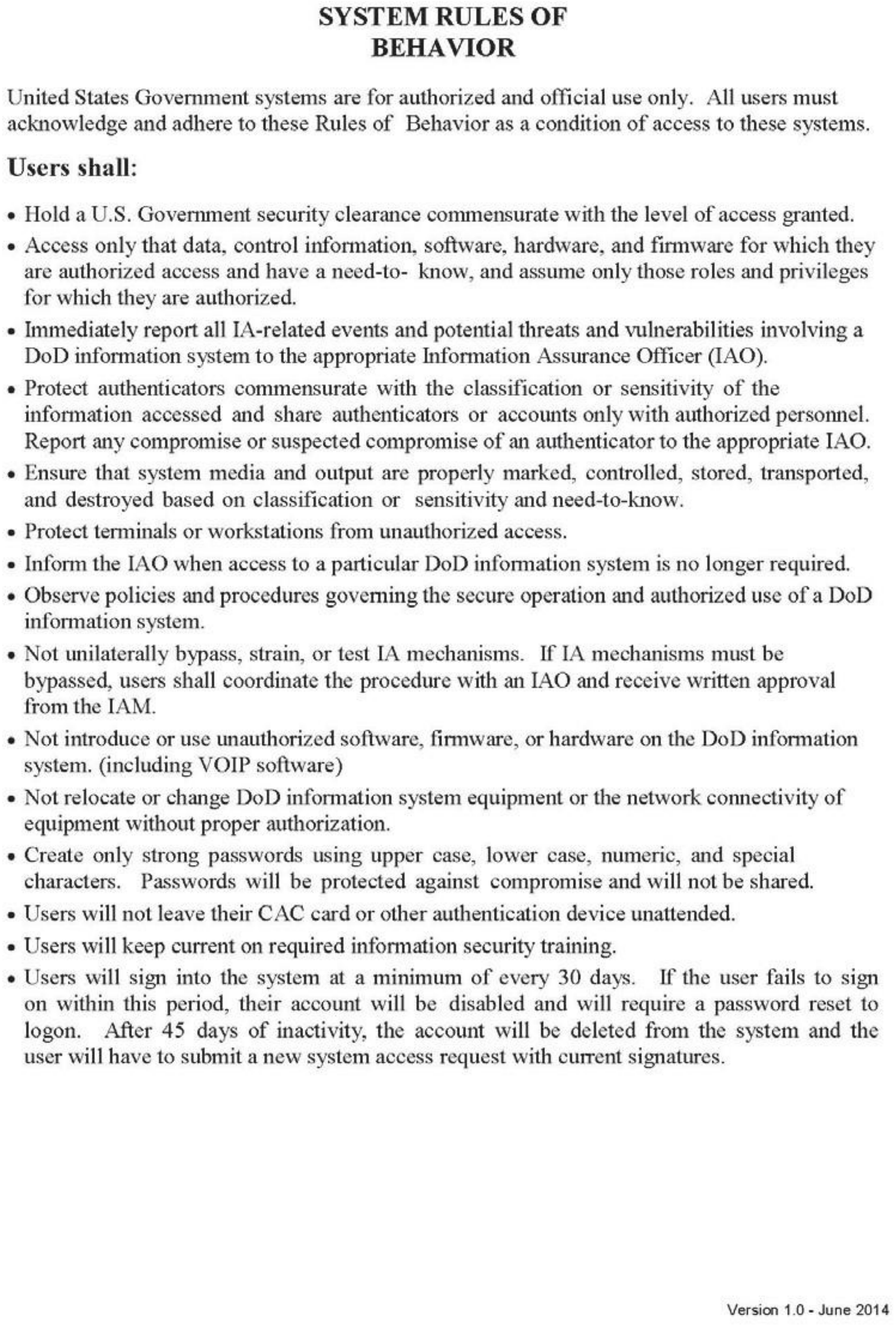
TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED *(YYYYMMDD)*	PROCESSED BY *(Print name and sign)*	DATE *(YYYYMMDD)*
DATE REVALIDATED *(YYYYMMDD)*	REVALIDATED BY *(Print name and sign)*	DATE *(YYYYMMDD)*

DD FORM 2875 (BACK), AUG 2009

Reset

System Authorization Access Request (DD FORM 2875, AUG 2009) SAMIS/AFSAC Online/Report.Web (FeTODS/ETOs/ITOs)

Example of Completed DD Form 2875 (continued):



SYSTEM RULES OF BEHAVIOR

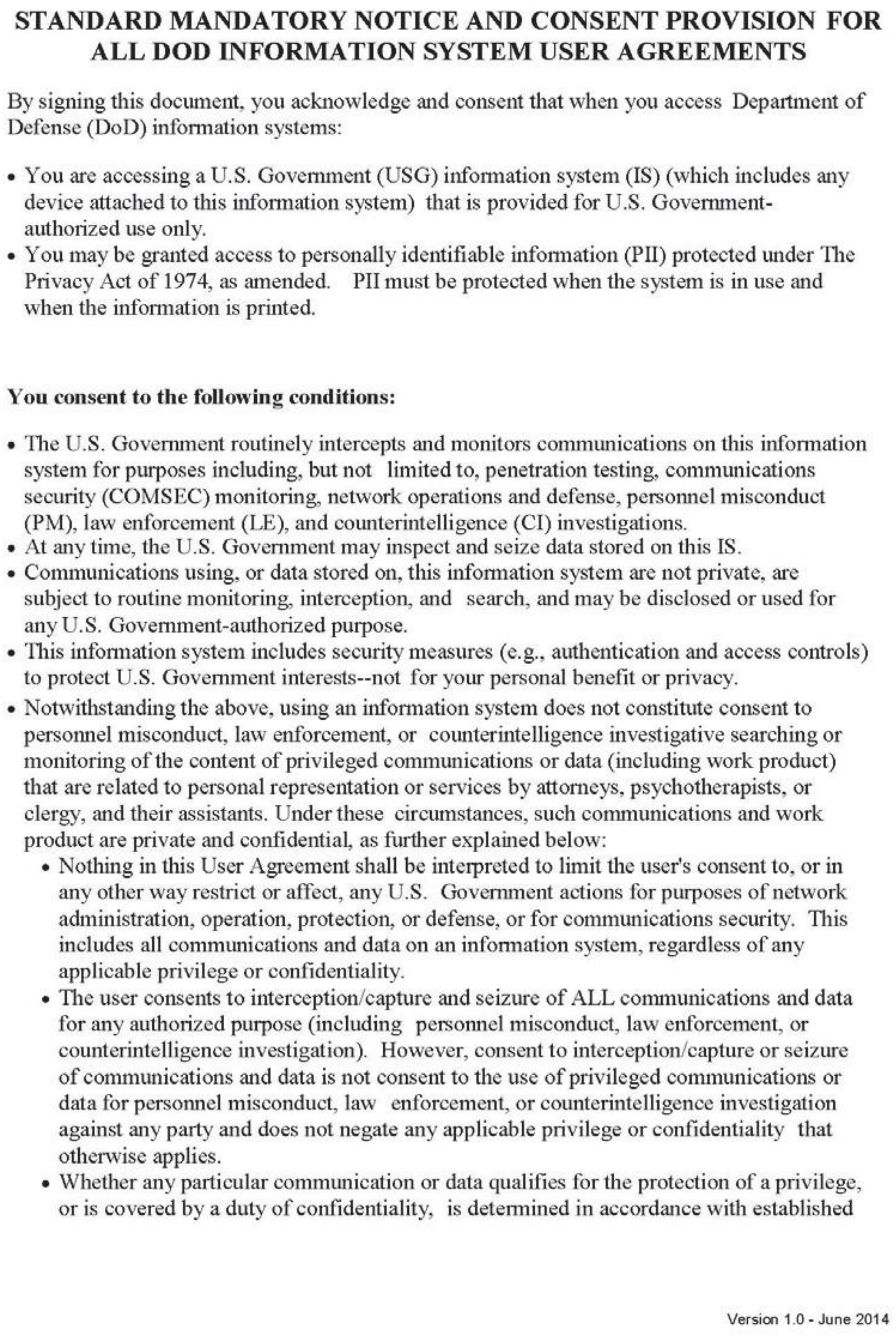
United States Government systems are for authorized and official use only. All users must acknowledge and adhere to these Rules of Behavior as a condition of access to these systems.

Users shall:

- Hold a U.S. Government security clearance commensurate with the level of access granted.
- Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to- know, and assume only those roles and privileges for which they are authorized.
- Immediately report all IA-related events and potential threats and vulnerabilities involving a DoD information system to the appropriate Information Assurance Officer (IAO).
- Protect authenticators commensurate with the classification or sensitivity of the information accessed and share authenticators or accounts only with authorized personnel. Report any compromise or suspected compromise of an authenticator to the appropriate IAO.
- Ensure that system media and output are properly marked, controlled, stored, transported, and destroyed based on classification or sensitivity and need-to-know.
- Protect terminals or workstations from unauthorized access.
- Inform the IAO when access to a particular DoD information system is no longer required.
- Observe policies and procedures governing the secure operation and authorized use of a DoD information system.
- Not unilaterally bypass, strain, or test IA mechanisms. If IA mechanisms must be bypassed, users shall coordinate the procedure with an IAO and receive written approval from the IAM.
- Not introduce or use unauthorized software, firmware, or hardware on the DoD information system. (including VOIP software)
- Not relocate or change DoD information system equipment or the network connectivity of equipment without proper authorization.
- Create only strong passwords using upper case, lower case, numeric, and special characters. Passwords will be protected against compromise and will not be shared.
- Users will not leave their CAC card or other authentication device unattended.
- Users will keep current on required information security training.
- Users will sign into the system at a minimum of every 30 days. If the user fails to sign on within this period, their account will be disabled and will require a password reset to logon. After 45 days of inactivity, the account will be deleted from the system and the user will have to submit a new system access request with current signatures.

System Authorization Access Request (DD FORM 2875, AUG 2009) SAMIS/AFSAC Online/Report.Web (FeTODS/ETOs/ITOs)

Example of Completed DD Form 2875 (continued):



STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.
- You may be granted access to personally identifiable information (PII) protected under The Privacy Act of 1974, as amended. PII must be protected when the system is in use and when the information is printed.

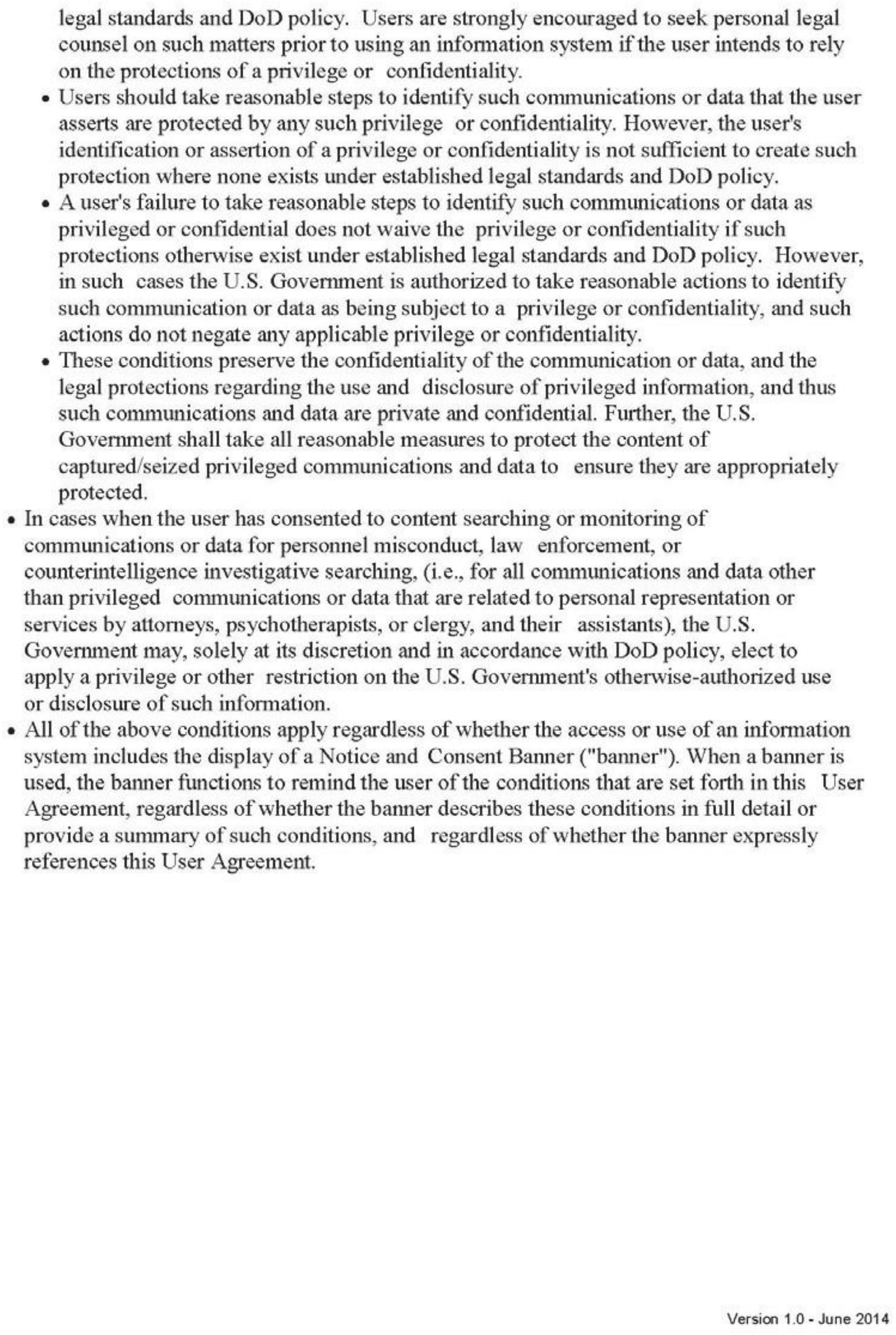
You consent to the following conditions:

- The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the U.S. Government may inspect and seize data stored on this IS.
- Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
- This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.
- Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
  - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
  - The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
  - Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established

Version 1.0 - June 2014

System Authorization Access Request (DD FORM 2875, AUG 2009) SAMIS/AFSAC Online/Report.Web (FeTODS/ETOs/ITOs)

Example of Completed DD Form 2875 (continued):



legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

  - Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
  - A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
  - These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

- In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
- All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provide a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.