

Complete sections as described in Item 9.

REQUEST FOR USER REGISTRATION ON THE SECURITY POLICY AUTOMATION NETWORK (SPAN)

SECTION A. USER INFORMATION

1. TITLE (Mr. Ms. Mrs.)/GRADE	2. NAME (Last, First, MI)	3. COMMERCIAL PHONE #
4. CLASS ACCOUNT UNCLASS ACCOUNT	5. <input type="checkbox"/> NEW ACCOUNT <input type="checkbox"/> EXISTING ACCOUNT <input type="checkbox"/> DELETE ACCOUNT	
6. OFFICE MAILING ADDRESS		
<input type="checkbox"/> SIPRNET EMAIL: <input type="checkbox"/> NIPRNET EMAIL: <input type="checkbox"/> SITE LOCATION _____		
7. SECURITY CLEARANCE (Circle One) TOP SECRET SECRET		
8. CONTRACTOR <input type="checkbox"/> YES IF YES, COMPANY NAME/ADDRESS (<i>ATTACH DISCLOSURE AGREEMENT</i>) <input type="checkbox"/> NO		
9. APPLICATION(S) REQUESTED		
<input type="checkbox"/> FOREIGN VISITS SYSTEM (FVS) – Complete sections A, B, and F. <input type="checkbox"/> USXPORTS – Complete sections A, C, D, and F. <input type="checkbox"/> FOREIGN DISCLOSURES SYSTEM (FDS) – Complete sections A, B, and F. (Requires signature of Foreign Disclosure Officer and approval of functions) <input type="checkbox"/> DOD PATENT APPLICATION REVIEW SYSTEM (DPARS) Complete sections A, E, and F <input type="checkbox"/> FOREIGN VISITS SYSTEM – CONFIRMATION MODULE (FVS-CM) Complete sections A and F		
10. SUPERVISOR NAME (Last, First)	11. SUPERVISOR PHONE #	
12. SUPERVISOR EMAIL ADDRESS		

SECTION B. FVS AND FDS PERMISSIONS

13. PLEASE INDICATE SYSTEM USAGE BELOW (see instructions)

- FOREIGN VISITS SYSTEM (FVS) COUNTRY DESK RESPONSIBILITY:**

Circle codes of country of responsibility: ALL 37 AG AJ AM AR AS AU BA BE BG BL BM BN BO BR BU CA CE CG CH CI CM CO DA DR EC EG EI EN ES EZ FI FK FM FR GB GE GG GH GM GR GT GV HA HO HU IC ID IN IR IS IT IV IZ JA JO KE KG KS KU KZ LG LH LO MD MO MU MX MY NI NL NO NP NT NZ PA PE PK PL PO PS QA RM RO RP RS SA SF SG SI SN SO SP SU SW SZ TC TH TI TS TU TX UK UP UR UY UZ VE WZ YE YO ZI Other: _____

- FOREIGN DISCLOSURE & FOREIGN VISITS SYSTEM PERMISSIONS:** Place an "x" in the appropriate boxes to indicate the functions the user is authorized to perform for each data base.

- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|--|-----|-----|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|-----|-----|--|--|--|--|--|--|
| <u>CASE PROCESSING</u>
1. CREATE/EDIT/COPY CASE
2. DELETE
3. ASSIGN/DEASSIGN
4. CLOSE
5. SAVE/REOPEN
6. CREATE/EDIT HISTORIC
7. OPEN/READ

<u>POSITION PROCESSING</u>
1. CREATE/EDIT POSITION
2. RELEASE
3. OPEN/READ | <table border="1" style="width:100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">FVS</td> <td style="width: 50%; text-align: center;">FDS</td> </tr> <tr><td> </td><td> </td></tr> <tr> <td style="text-align: center;">FVS</td> <td style="text-align: center;">FDS</td> </tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> </table> | FVS | FDS | | | | | | | | | | | | | | | | | | | FVS | FDS | | | | | | |
| FVS | FDS | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FVS | FDS | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

SECTION F. AUTHORIZATION

4. I HEREBY CERTIFY THAT THE USER AND PROJECT OFFICER INFORMATION SHOWN ABOVE IS CORRECT AND THAT THE USER HAS A BONAFIDE NEED TO USE THE INDICATED APPLICATION AND RELATED FUNCTIONS AND IS A U.S. CITIZEN.

(Signature of Security Manager) Date

(Signature of Supervisor) Date

(Signature of Foreign Disclosure Officer) Date

SECTION G. DTSA FUNCTIONAL MANAGER SIGNATURES

DTSA Functional Manager (FVS) Date

DTSA Functional Manager (USXPORTS) Date

DTSA Functional Manager (FDS) Date

DTSA Functional Manager (DPARS) Date

*******DEFENSE TECHNOLOGY SECURITY ADMINISTRATION USE ONLY*******

USERID _____

DIRECTORY _____

OFFICE _____

ORGANIZATION _____

AGENCY _____

INSTRUCTIONS FOR COMPLETION OF REQUEST FOR
USER REGISTRATION ON THE SECURITY POLICY AUTOMATION NETWORK (SPAN)

SECTION A. USER INFORMATION: Complete Blocks 1 through 12.

- Block 7 - Ensure Clearance is reflected. SECRET is required for SPAN access.
- Block 8 - If the user is a contractor, the individual must attach a SPAN Contractor Disclosure Agreement to this request.

SECTION B. FVS AND FDS PERMISSIONS: Block 13.

All users receive Open/Read permissions for Foreign Visits and Foreign Disclosure.

Foreign Visits: Circle all countries this user is responsible for. Most users in subordinate organizations receive permissions to “ALL” countries.

Foreign Disclosure Information: By authorizing these permissions, (see descriptions below: Case Processing and Position Processing), this user may accomplish the following case and position processing capabilities for the office the individual is assigned to. FDS is the Classified Military Information.

CASE Processing: (primarily for Office of Primary Responsibility (OPRs))

1. CREATE/EDIT/COPY Case: Originate a case, EDIT the information, and COPY information for creation of similar cases.
2. DELETE: Completely eliminate a case from the system provided the individual deleting is a member of the organization that originally created it.
3. ASSIGN/DEASSIGN: Allows staffing to other organizations.
4. CLOSE: CLOSEs a case to further input. Changes case status from OPEN to CLOSED.
5. SAVE/REOPEN: SAVE is the quality assurance step and changes case status from CLOSED to SAVED. REOPEN allows a CLOSED or SAVED case to return to OPEN status for updating.
6. CREATE/EDIT HISTORIC: Allows case creation or editing of a case in the historic data base. Both permissions are accomplished with a SAVED case status.

POSITION Processing:

1. CREATE/EDIT Position: Enter or change a position, provided it has not yet been released.
2. RELEASE: Signifies the position represents the organization’s official recommendation in a specified case. Allows viewing by other organizations. RELEASE function permissions are usually limited to selected individuals.

SECTION C. USXPORTS ORGANIZATION INFORMATION

USXPORTS users must supply the organizations to which they belong. For each organization, the organization code and the parent organization must be supplied.

INSTRUCTIONS FOR COMPLETION OF REQUEST FOR
USER REGISTRATION ON THE SECURITY POLICY AUTOMATION NETWORK (SPAN)

SECTION D. USXPORTS PERMISSIONS

All users have access to FMS cases.

Indicate the desired Case Processing permissions in the following checkboxes for CCL, MUN, or EC Cases. Organization Administration (OA) and Maintain Policy Assessment Repository (MIR) permissions do not require a case type; the N/A column should be marked to indicate these permissions.

1. DUTT (Dual-Use Tiger Team): Provides access to the Tiger Team area; allows loading/viewing of Dual-Use Cases assigned to the Tiger Team.
2. MUNTT (Munitions Tiger Team): Provides access to the Tiger Team area; allows loading/viewing of Munitions Cases assigned to the Tiger Team.
3. RDP (Release DoD Position): Allows users to release the DoD Position on a case.
4. RP (Release Position): Allows the user to release the Organization's position.
5. USG (Create/Edit USG Position). Allows the user to create/edit a USG Position for a case when an electronic USG Position is not received.
6. DRP (Directly Release Positions): Allows Sr. NON OPRS and NON OPRS to release a position without having to go through the normal SSO/RO signature process.
7. This permission does not apply to OPRs.
8. CC (Create Case): Allows the creation of Cases; editing/deleting of Case elements such as Parties, Commodities, Documents, etc.; deletion of Cases prior to "Completion"; and Completion of Cases.
9. ROC (Reopen Case): Allows the user to reopen/reclose Munitions cases.
10. DEC (Deassign Case): Allows the user to remove an assignment from a case.
11. MIR (Maintain Policy Assessment Repository): Allows user maintenance rights in the Policy Assessment Repository.
12. OA (Organization Administration): Allows the user to conduct certain Organization level maintenance tasks, such as maintaining Organization Standard Language, Organization Geographical Groups, and Organization Reference Library documents.
13. AA (Application Administration): Allows the user to conduct certain Application level maintenance tasks, such as maintaining/assigning permissions, maintaining reference tables, etc.
14. AU (Audit User): Allows the user to see all Positions, Comments, Annotations, Assignments, etc. on a given Case (normally these are restricted by various viewing rules based on the User's Organization).
15. COTU (Create One-Time User): Allows the user to create a "one-time" user account.
16. SR (Schedule Reports): Allows the user to schedule reports.
17. RNOR (Run Non-OPR Reports): Allows the user to generate reports that are restricted to non-OPR users.
18. ROR (Run OPR Reports): Allows the user to generate reports that are restricted to OPR users.
19. DEFAULT (Default Set of Permissions): Assigns the general default set of permissions to the user.

SECTION E. DPARS PROFILE:

SERVICE/AGENCY: Select the service or agency that your organization falls under.

ROLE: Select if your role will be Military Department Reviewer or Field Evaluation Site Reviewer.

FIELD EVALUATION SITE: Enter your field evaluation site full name and acronym.

ADDITIONAL COMMENTS: Enter your request for user ID and password.

SECTION F. AUTHORIZATION: Block 14. The Security Manager and user's supervisor MUST sign this block. The Security Manager must ensure the security clearance in Block 7 is correct. The FDO must sign if FDS is requested. All must approve the application and related functions.

Send the completed form to DTSA SPAN Support, 4800 Mark Center Dr., Suite 7F09-02, Alexandria, VA 22350-1600 or fax it to 571-372-2589. Upon receipt, SPAN Support will arrange training and issue a password for access to the Security Policy Automation Network.

APPENDIX I - CONTRACTOR DISCLOSURE STATEMENT

SECURITY POLICY AUTOMATION NETWORK

Date: _____

MEMORANDUM FOR CIO, DEFENSE TECHNOLOGY SECURITY ADMINISTRATION
(DTSA)

SUBJECT: Statement of Disclosure

This memorandum notifies you that, as a contractor, I require access to a Security Policy Automation Network (SPAN) workstation to perform duties as assigned.

I will attend an unclassified briefing on the SPAN to understand the requirement to safeguard and protect DoD information and property and will use the network and automated information systems for official purposes only.

I will not search, retrieve, or read proprietary information or classified information for the purposes of information gathering for self interests. I understand that any violation of this integrity statement will be reported to DTSA Physical Security.

I will report to the Security Officer all security violations or deviations.

I have no unanswered questions about my responsibilities.

I request user registration on SPAN and the issuance of appropriate user ID and password.

_____ (signature)

_____ (printed name)

_____ (company)