

APPLICATION

FOR

GIDEP PARTICIPATION

REQUIRED DOCUMENTATION FOR MEMBERSHIP

YOU MUST SUBMIT:

- 1. Completed GIDEP Participation Request Form**
- 2. Completed GIDEP User Authorization Form**
- 3. For Government Contractors/Subcontractors, Proof of Business with the US or Canadian Government with one of the following:**
 - Copy of Government contract**
 - Copy of purchase order with Government Contractor**

SEND DOCUMENTATION TO:

GIDEP Operations Center, P. O. Box 8000 Corona, CA 92878-8000

OR

FAX: (951) 898-3250

OR

EMAIL: roster@gidep.org

GIDEP PARTICIPATION REQUEST

**Reserved for
Office Use Only**

GIDEP Operations Center
Approval Officer
APPROVED: _____
DENIED: _____
DATE: _____

We hereby request participation in GIDEP and agree to abide by the GIDEP Participation Requirements shown below.

The **company/activity official** authorizing participation is:

Name (Last, First, M.I.): _____

Position Title: _____

Signature: _____

Phone: _____

Our appointed **GIDEP Representative** will be:

Name (Last, First, M.I.) _____

Position Title: _____

Activity/Company: _____

Mailing Address: _____

City, State, Zip _____

Nature of Business: _____

Telephone number: (____) _____

FAX number: (____) _____

E-mail Address: _____

Note! This application may be stored electronically and the scanned signature will be treated as an original signature.

Send this form together with at least one GIDEP User Authorization form to:

GIDEP Operations Center, P. O. Box 8000 Corona, CA 92878-8000 OR

FAX: (951) 898-3250 OR EMAIL: roster@gidep.org

GIDEP PARTICIPATION REQUIREMENTS

ELIGIBILITY Only the following types of activities are eligible for GIDEP participation:

- a. An U. S. Government agency.
- b. An agency of the Canadian Department of National Defence.
- c. An U. S. or Canadian business organization that directly or indirectly provides equipment, material, or services under U. S. or Canadian government contract.
- d. A licensed U. S. public utilities company.

TERMS AND CONDITIONS GIDEP information is provided on a **privileged** basis. Participants must agree to the following terms and conditions:

- a. Dissemination and utilization of GIDEP information is limited to participants.
- b. GIDEP participants must safeguard GIDEP data in accordance with the Security and Technology Transfer restrictions of the U. S. Government.
- c. GIDEP participants must obtain permission from the document originator or the GIDEP Program Manager prior to releasing information to non-participants.
- d. GIDEP participants must control access to the GIDEP WEB database.
- e. GIDEP participants must follow the Information Security Policy shown on GIDEP User Authorization form.
- f. GIDEP participants must return GIDEP materials if participation is terminated.

REQUIREMENTS The following requirements apply to all eligible participants. The participating activity must:

- a. Support and promote the GIDEP mission.
- b. Designate, in writing, a GIDEP Representative and persons that will be using the GIDEP database.
- c. Establish in-house procedures for utilization of GIDEP.
- d. Submit documents for inclusion in the GIDEP database.
- e. Submit a **Utilization Report** at least once annually.

COST Participants are responsible for their own in-house costs, including labor, equipment, and Internet access and/or phone (modem).

POLICIES AND PROCEDURES The above participation requirements are excerpted from the GIDEP Operations Manual.

GIDEP USER AUTHORIZATION
(ONE FORM IS REQUIRED FOR EACH GIDEP DATABASE USER)

By signing this authorization, I certify that I AM an employee of the participating activity/company and that I:

1. Have read and understand the Information Security Policy below dated 2 August 1999.
2. Agree to comply with the terms and conditions of the Policy shown below.

1. USER NAME (TYPE OR PRINT):	2. DEPT/MS:	3. PHONE: ()
4. JOB TITLE	5. E-MAIL ADDRESS:	
6. ORGANIZATION:		7. PARTICIPANT CODE: (if assigned)
8. SIGNATURE:		9. CITY OF BIRTH (for security use only):
10. PRIMARY AREA(S) OF INTEREST: (Select all that apply.)		
<input type="checkbox"/> Engineering Data	<input type="checkbox"/> Failure Experience Data	<input type="checkbox"/> Reliability Maintainability Data
<input type="checkbox"/> Metrology Data	<input type="checkbox"/> Product Information Data (DMS/MS)	
11. HOW DID YOU HEAR ABOUT GIDEP? (Select all that apply.)		
<input type="checkbox"/> World Wide Web	<input type="checkbox"/> Exhibit/Show _____	<input type="checkbox"/> Clinic _____ (Year)
<input type="checkbox"/> GIDEP Representative	<input type="checkbox"/> GIDEP Workshop _____	(Year / Location)
<input type="checkbox"/> Contractor _____	<input type="checkbox"/> GROW _____	<input type="checkbox"/> OTHER _____
THIS PART MUST BE COMPLETED BY THE GIDEP REPRESENTATIVE		
12. GIDEP Push Mail: The above GIDEP User is approved to receive push-mail. <input type="checkbox"/> YES <input type="checkbox"/> NO		
By signing this authorization, I support, as the GIDEP REPRESENTATIVE, the policies and procedures stated in the INFORMATION SECURITY POLICY. I will also notify the GIDEP Operations Center if the above GIDEP user no longer requires access to the GIDEP databases.		
13. GIDEP REPRESENTATIVE (TYPE OR PRINT):		14. DATE:
15. SIGNATURE:		

This application may be stored electronically and the scanned signature will be treated as an original signature.

INFORMATION SECURITY POLICY

2 August 1999

Purpose: To make known general Automated Information Systems (AIS) security guidelines for accessing databases where communication is via approved Internet web to U. S. Government (NAVY) computer systems.

Scope: These procedures set forth the basic AIS security protocol for signing-on, signing-off and general use of the host computer system. These security guidelines comply with DoD Manual 5220.22M and OPNAVINST 5239.1A. Access to GIDEP information is controlled through a series of good operating practices and privileged passwords assigned to authorized users. Misuse of passwords and the access obtained by their usage can result in denial of further GIDEP usage and possible penalties under 18 USC 1905 and other applicable statutory regulations.

Password Control The GIDEP representative for each participating activity will submit a GIDEP USER AUTHORIZATION (GUA) form for each user to the GIDEP Operations Center. The GIDEP Operations Center will issue a temporary password for each new user identified on the GUA. This password is valid for a period of fifteen (15) days and must be changed by the user before accessing the GIDEP database. The password should be changed at three to six month intervals, but no longer than six months, or anytime actual or suspected compromise of the password has occurred. When the user resigns, has been terminated, transfers, or has no further authorized use for his/her passwords, immediately notify the GIDEP Operations Center Help Desk by e-mail (roster@gidep.org) or Phone (951) 898-3207.

Do NOT share your passwords. You are responsible for all activity initiated under your password.

Do NOT leave the computer unattended when logged on to GIDEP. Terminate web access when a session is completed. Report suspected tampering or security violations to the company security personnel and the GIDEP Operations Center. Stop processing data until the system can be checked.

Data Management Do not process classified information. Protect all GIDEP information (hard copy and electronic media) from unauthorized disclosure. If in doubt about proper security procedures, please contact your security manager and/or the GIDEP Operations Center for further assistance or information.