



West Virginia National Guard

Human Resources Office

Bulletin



Bulletin Number: 18-01

Date: 27 February 2018

Applicability: WVNG Activity Heads and Human Resources (HR) Remotes who have technician responsibilities

DCPDS Deployment

Subject: Extension of the Defense Civilian Personnel Data System (DCPDS) to the field

References: Guide for the Human Resources Specialist (Information Systems) Operations, Appendix F-10; Information Paper, NGB-TNI dated 8 June 2004

Effective Date: 27 February 2018

Use: This bulletin provides basic guidance to activity heads and Human Resources Remotes to ensure the seamless transition of deploying DCPDS access beyond HRO (Human Resources Office) personnel.

Introduction and Background:

The Office of Technician Personnel, Information Systems Branch (NGB-J1-TNI) is responsible for program management of DCPDS which migrated to a web-based system in 2003. Most recently, DCPDS is available for key personnel outside the WVNG HRO. The WVNG HRO is preparing to extend the availability of DCPDS to designated individuals at each activity head to enable more efficient, effective processing and tracking of technician personnel actions.

The HRO shall remain the primary processing center for all personnel actions and The Adjutant General will remain as the overall approval authority for all technician personnel actions. All Requests for Personnel Action, Standard Form (SF) 52s, will be electronically transmitted through DCPDS to the HRO. The HRO will make the determination whether the action is approved to be processed and if so, obtain The Adjutant General's final approval on the requested action.

Overview: DCPDS will be deployed to select personnel in the field to enable better visibility and will expedite processing of technician personnel actions. Appropriate personnel will be identified within each activity head. Appropriate group boxes will be created by the DCPDS helpdesk. Training will be conducted for all identified and approved personnel. Deployment will be implemented within the WVNG technician program. Upon the DCPDS deployment, no paper/electronic SF 52s will be accepted by HRO for technician personnel actions.

NOTE: The activity head's current internal process of routing SF 52s will not be impacted/changed. The only part of the process that changes is instead of providing a paper SF 52 to HRO, the Initiator will put the information directly in to DCPDS.

Immediate Action: All HRO extension personnel (i.e. Activity Heads, Remote Designees, liaisons, etc.) will receive a memorandum identifying personnel who will assume the responsibility of the appropriate DCPDS deployment role and respond within the identified timeframe. The respective activity head will review and approve the memorandums. If the respective unit makes additions or corrections to those personnel identified, explicit supporting documentation must be provided to the HRO to justify the change.

Once designated personnel are approved by the Activity Head, a System Authorization Access Request (SAAR), SF 2875, must be completed and returned to HRS-IS. (See attached example.) DCPDS account access will NOT be granted unless the proper, completed documentation is received.

Future Changes: As personnel changes occur, the memorandum must be updated appropriately and signed by the activity head and forwarded to the HRO.

Roles and Responsibilities:

Initiator – Person(s) identified via memorandum/appointment letter who enter(s) personnel actions in to DCPDS.

Reviewer – Person(s) identified via memorandum/appointment letter who simply review(s) personnel actions prior to final approval in DCPDS.

Authorizer – Person(s) identified via memorandum/appointment letter who overall approve(s) the requested personnel actions in DCPDS on behalf of the Activity Head.

Activity Head – Person responsible for identifying/confirming DCPDS roles and notifying the HRO, HRS-IS when personnel changes occur.

HRS-IS – Primary HRO POC for training Initiators, Reviewers and Authorizers. Primarily responsible for maintaining user accounts (creation and deletion.)

Classification – Primary HRO POC for questions regarding position information.

Staffing – Primary HRO POC for questions regarding personnel and pay information.

Benefits – Primary HRO POC for questions regarding benefit and retirement/separation information.

Your points of contact are the Technician Hotline at (304)561-6749 for questions regarding the specific areas mentioned above and HRS-IS at (304)561-6427 for questions regarding DCPDS access.



DAVID P. SHAFER
COL, EN, WVARNG
Human Resource Officer

Encl

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 <input checked="" type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID _____	DATE (YYYYMMDD) 20170801
--	------------------------------------

SYSTEM NAME (Platform or Applications) Oracle Application	LOCATION (Physical Location of System) _____
---	--

PART I (To be completed by Requestor)

1. NAME (Last, First, Middle Initial) Smith, Joe A.	2. ORGANIZATION JFHQ-WV-HRO
3. OFFICE SYMBOL/DEPARTMENT HRO/IS	4. PHONE (DSN or Commercial) 623-6427
5. OFFICIAL E-MAIL ADDRESS joe.smith@ang.af.mil	6. JOB TITLE AND GRADE/RANK Human Resources Specialist (Info Sys) GS-09
7. OFFICIAL MAILING ADDRESS 1703 Coonskin Drive Charleston, WV 25311	8. CITIZENSHIP <input checked="" type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER
9. DESIGNATION OF PERSON <input checked="" type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR	
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) <input checked="" type="checkbox"/> I have completed Annual Information Awareness Training. DATE (YYYYMMDD) 20091005	

11. USER SIGNATURE Joe A. Smith	12. DATE (YYYYMMDD) 20170620
---	--

GRAY.MEREDITH.A.105
 2341473
Digitally signed by GRAY.MEREDITH.A.1052341473
 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
 ou=USAF, cn=GRAY.MEREDITH.A.1052341473
 Date: 2017.06.14 09:38:52 -0400

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
 User requires DCPDS access for everyday job functions.

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. <input checked="" type="checkbox"/>	16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.) _____
---	--

17. SUPERVISOR'S NAME (Print Name) Joe A. Supervisor	18. SUPERVISOR'S SIGNATURE GRAY.MEREDITH.A.1052341473 <small>Digitally signed by GRAY.MEREDITH.A.1052341473 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USAF, cn=GRAY.MEREDITH.A.1052341473 Date: 2017.06.14 09:39:57 -0400</small>	19. DATE (YYYYMMDD) 20170620
--	---	--

20. SUPERVISOR'S ORGANIZATION/DEPARTMENT JFHQ-WV-HRO Information Systems	20a. SUPERVISOR'S E-MAIL ADDRESS joe.a.supervisor.mil@mail.mil	20b. PHONE NUMBER (304) 561-6427
---	--	--

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) _____
---	---	----------------------------------	-------------------------------------

26. NAME (Last, First, Middle Initial) Smith, Joe A.
27. OPTIONAL INFORMATION (Additional information)

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

28. TYPE OF INVESTIGATION SAC	28a. DATE OF INVESTIGATION (YYYYMMDD) 20100511		
28b. CLEARANCE LEVEL Secret	28c. IT LEVEL DESIGNATION <input type="checkbox"/> LEVEL I <input type="checkbox"/> LEVEL II <input checked="" type="checkbox"/> LEVEL III		
29. VERIFIED BY (Print name) Joe A. Security	30. SECURITY MANAGER TELEPHONE NUMBER (304) 561-6427	31. SECURITY MANAGER SIGNATURE GRAY.MEREDITH.A <small>Digitally signed by GRAY MEREDITH A 1052341473 DN: cn=US, o=U.S. Government, ou=DO, c=US, ou=USAP, cn=GRAY.MEREDITH.A.1052341473 Date: 2017.06.14 09:41:42 -0400</small>	32. DATE (YYYYMMDD) 20160622

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 or modifying 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 number.
- (5) Official E-mail Address. The user's official e-mail address.
- (6) Job Title/Grade/Rank. The civilian job title (Example: Systems Analyst, GS-14, Pay Clerk, GS-5)/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).
- (9) Designation of Person (Military, Civilian, Contractor).
- (10) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness 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 if less than 1 year.
- (17) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.
- (18) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.
- (19) Date. Date supervisor signs the form.
- (20) Supervisor's Organization/Department. Supervisor's organization and department.
- (20a) E-mail Address. Supervisor's e-mail address.
- (20b) Phone Number. Supervisor's telephone number.

(21) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.

(21a) Phone Number. Functional appointee telephone number.

(21b) Date. The date the functional appointee signs the DD Form 2875.

(22) Signature of Information Assurance Officer (IAO) or Appointee. Signature of the IAO or Appointee of the office responsible for approving access to the system being requested.

(23) Organization/Department. IAO's organization and department.

(24) Phone Number. IAO's telephone number.

(25) Date. The date IAO signs the DD Form 2875.

(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 (Secret or Top 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) Security Manager Telephone Number. The telephone 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 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.