Navy
Official Military Personnel File
(OMPF) - Administrator (Admin) Access
and
OMPF - Command View
Users' Guide

Version 1.0

7 January 2011

Navy Personnel Command

Personnel Information Management Department

5720 Integrity Drive

Millington, TN 38055-7400

Support provided by:

Functional Requirements Group

Table of Contents

Table of Figures

Record of Changes

Change Number	Date	Entered By	Reason for Change
1	7 Jan 2011	D. Gemuend	Modify email address

1 Overview

This document contains diagrams and narratives relating to the Navy's Official Military Personnel File (OMPF) – Administrator Access and OMPF-Command View external user interface applications.

- OMPF – Command View Application.
    - Provides command-level access to Official Military Personnel Files (OMPFs) maintained at Navy Personnel Command
    - Access to OMPFs limited within Access Control Lists (ACLs) set on:
        - Command/Administrative UIC hierarchies
        - Personnel office/supported customer UICs
        - Admin UICs/supported Reserve UICs
- OMPF – Administrator (Admin) Access Application.
    - Online tool to be used by designated command personnel to administer and manage OMPF view roles.

The objectives:

- Support the elimination of the Enlisted Field Service Record
- Short-term solution to provide access to legacy Officer and Enlisted record information not available in the Electronic Service Record (ESR) and Career Information Management System (CIMS) modules within Navy Standard Integrated Personnel System (NSIPS), and other official data sources such as the Enlisted Distribution Verification Report (EDVR).
- Comply with the Government Paperwork Elimination Act (GPEA) of 1998 that mandates Federal agencies to maintain records electronically, when practicable.
- Provide security and protection of Protected Personal Information (PPI).
- Improve the Navy's personnel record maintenance business process.
- Augment official personnel data sources when information is not otherwise available.

1.1 Protection of Official Military Personnel Files (OMPFs) Information

The Navy's single authoritative Official Military Personnel Files (OMPFs) are maintained by Navy Personnel Command (CNPC) in the Electronic Military Personnel Records System (EMPRS) as required by federal statute and current Department of Defense and Navy directives. The OMPF is the Sailor's permanent personnel record documenting their career from accession to discharge or retirement.

- All military personnel record information is classified as **"For Official Use Only"** with Protected Personal Information (PPI) covered by the Privacy Act. Personnel entrusted with access to OMPF information must have the appropriate active security investigation and should be familiar with the references listed in the appendix of this guide.

- **All authorized users** of the OMPF – Administrator Access and/or OMPF- Command View applications **must** have a current System Authorization Access Request – Navy form (SAAR-N) (OPNAV FORM 5239/14), **and** a current and approved NAVPERS 1070/857, Request for Access to Electronic Military Personnel Records System (EMPRS) on file with the command's Information Assurance or Security Manager. *Refer to Chapters 5.1 and 5.2 for guidelines as to the completion and retention of both forms.*

- All authorized users of both applications must have access to BUPERS Online (BOL). *Refer to Chapter 5.1 for guidelines to request access to BOL.*

- Personnel data is to be accessed and/or used **only** for official actions in the performance of personnel administrative tasks and is only to be disclosed to authorized persons conducting official military business.

- Individuals with proper clearance investigations and authority to view record information will not permit unauthorized access to record information, and must ensure adequate safeguards enforcement to prevent disclosure of record information.

- Misuse of record information due to loose interpretation of "official actions in the performance of personnel administrative tasks" can result in the spillage of Personal Protected Information (PPI). Unless specifically required by an official directive, record documents will not be provided as part of routine nomination or screening packages.

- The Privacy Act of 1974 (Title 5, U.S.C., Section 552a) provides for criminal penalties against anyone who discloses information to unauthorized persons. Anyone who obtains information about an individual under false pretences may also be subject to criminal penalties.

2 OMPF-Admin Access and OMPF-Command View Roles

	Role Authorized Actions	*Admin Access	* Delegated Admin	Command View	Command-Only View
For Onboard UIC					
OMPF-Admin Access	Assign/Unassigned - Delegated Admin Users	X			
	Assign/Unassigned - Command View Users	X	X		
	Assign/Unassigned - Command-Only View Users	X	X		
OMPF-Command View	View OMPF documents	X	X	X	X
	Print OMPF documents	X	X	X	X
	Download OMPF documents	X	X	X	X
For Subordinate UICs					
OMPF-Admin Access	Assign/Unassigned - Delegated Admin Users	X			
	Assign/Unassigned - Command View Users	X	X		
	Assign/Unassigned - Command-Only View Users	X	X		
OMPF-Command View	View OMPF documents	X	X	X	
	Print OMPF documents	X	X	X	
	Download OMPF documents	X	X	X	

* Admin / Delegated Admin Users must be E6 & above

Figure 2-1: OMPF- Admin Access and Command View Role Matrix

There are four user roles for the OMPF-Admin Access and OMPF-Command View applications with different levels of access as depicted in the Role Matrix provided in figure 2-1.

1. **Administrator or Admin Access Role**.

   a. Applications Access. Admin Access users have automatic access based on the following:

      1) Flag Officers – continuous access based on rank

      2) Commanding Officers, Executive Officers, Officers in Charge, Commanders, Deputy/Vice Commanders, Chiefs of Staff and Chief Staff Officers – upon assignment to a designated Billet Navy Officer Billet Classification listed in Table 1 of Appendix 6.1 of this guide. Access terminates upon transfer from the authorizing billet or removal of billet NOBC.

      3) Command Master Chiefs (to include Fleet and Force Master Chiefs), Command Senior Chiefs and Chiefs of the Boat – upon assignment to a designated Distribution Navy Enlisted Classifications (DNECs) listed in Table 2 of Appendix 6.1 of this guide. Access terminates upon loss of the DNEC.

b. OMPF - Admin Access Application. The Admin Access role will use the administrative tool to manage the roles of Delegated Admin, Command View and Command-Only View for their Unit Identification Code (UIC) Access Control List (ACL) hierarchy:

1) Personnel within their onboard Unit Identification Code (UIC)

2) Personnel within their administrative subordinate UICs as designated by the Standard Navy Distribution List (SNDL) (OPNAVNOTE 5400).

a) The Navy Activity Status (NAVACTSTAT) master file captures only the Major Command (Echelon II) and Sub-Major Command (Echelon III) for each activity. Therefore, the Echelon IVs will not have visibility of their subordinate UICs in this short-term solution. *Refer to Chapter 5.3 for corrections to the Administrative Shore or Fleet Chains of Command.*

b) Reserve Admin UICs will have the ability to manage the User roles of Delegated Admin, Command View and Command-Only View for the Reserve UICs (RUICs) within the area of responsibility (AOR) as designated in the Reserve Headquarters System (RHS).

3) Command UICs are limited to 10% (rounded down) of the Billets Authorized (BA) to be assigned as users within both applications. *Admin Access Users do not count against the command's total number of users.*

4) PSDs are limited to a total of 20 users who can be assigned as users within both applications.

c. OMPF- Command View Application. The Admin Access role will use the OMPF view application to view, print or download:

1) OPMF documents in "Non-controlled" Records within their onboard and subordinate UICs in the ACL.

a) Officer Admin Users – have access to documents in Officer Field Codes 01, 02, 04 through 16, 18 and 98 as well as Enlisted Field Codes 30 through 43, 45, and 99. *Refer to Appendices 6.3 and 6.4 for the list of Field Codes.*

b) Enlisted Admin Users – have access to documents in Enlisted Field Codes 30 through 43, 45, and 99

i) If assigned to a designated Personnel Support Detachment, the Admin Access User will also have access to the OMPFs for the UICs and Reserve UICs (RUICs) within the designated area of responsibility (AOR). *Appendix 6.1 lists the PSD UICs.*

ii) If assigned to a Reserve Admin UIC, the Admin Access User will also have access to the OMPFs for the Reserve UICs (RUICs) within the AOR as designated in RHS.

2. **Delegated Admin Access User**. Delegated Admin Access Users must be military E6 and above.

a. Applications Access.

1) Delegated Admin Users will be "delegated" access by an Admin Access User within the UIC or in the Echelon II or III command in the ACL.

a) Commands or UICs are limited to one (1) Delegated Admin Access User per 200 Billets Authorized (BA) (1:200).

b) Delegated Admin Users will request access using the guidelines provided in Chapter 5.2 in this guide.

c) Access will terminate…

i) upon transfer or separation from the UIC, or

ii) upon the assigning Admin Access User's loss of access, or

iii) upon access removal by an ACL Admin Access User.

2) PSD Delegated Admin Users will be "delegated" access by CNPC.

a) PSDs are limited to three (3) Delegated Admin Access Users within the PSD UIC.

b) PSD Delegated Admin Users will request access using the guidelines provided in Chapters 5.1 and 5.2 in this guide.

c) Access will terminate upon transfer or separation from the UIC, or when access is removed by CNPC.

3) Reserve UIC (RUIC) Delegated Admin Users will be "delegated" access by the Reserve Admin UIC Admin Access User.

a) Reserve Units or RUICs are limited to one (1) Delegated Admin User per 200 Billets Authorized (BA) (1:200).

b) Reserve Delegated Admin Users will request access using the guidelines provided in Chapter 5.2 in this guide.

c) Access will terminate…

i) upon transfer or separation from the RUIC, or

ii) upon the assigning Admin Access User's loss of access, or

iii) upon access removal by an ACL Admin Access User.

b. <u>OMPF - Admin Access Application</u>. The Delegated Admin role will use the administrative tool to manage the roles of Command View and Command-Only View for their ACL hierarchy:

1) Personnel within their onboard Unit Identification Code (UIC)

2) Personnel within their administrative subordinate UICs as designated by the Standard Navy Distribution List (SNDL) (OPNAVNOTE 5400)

a) The Navy Activity Status (NAVACTSTAT) master file captures only the Major Command (Echelon II) and Sub-Major Command (Echelon III) for each activity. Therefore, the Echelon IVs will not have visibility of their subordinate UICs in this short-term solution. *Refer to Chapter 5.3 for corrections to the Administrative Shore or Fleet Chains of Command.*

b) Reserve Admin UICs will have the ability to manage the User roles of Delegated Admin, Command View and Command-Only View for the Reserve UICs (RUICs) within the AOR as designated in RHS.

c. <u>OMPF- Command View Application</u>. The Delegated Admin role will use the OMPF view application to view, print or download:

1) OPMF documents in "Non-controlled" Records within their Admin ACL

a) Officer Delegated Admin Users – have access to documents in Officer Field Codes 01, 02, 04 through 16, 18 and 98 as well as Enlisted Field Codes 30 through 43, 45, and 99.

b) Enlisted Delegated Admin Users – have access to documents in Enlisted Field Codes 30 through 43, 45, and 99.

i) If assigned to a designated Personnel Support Detachment, the Delegated Admin User will also have access to the OMPFs for the UICs and/or Reserve UICs (RUICs) within the designated area of responsibility (AOR). *Appendix 6.2 lists the PSD UICs.*

ii) If assigned to a Reserve Admin UIC, the Admin Access User will also have access to the OMPFs for the Reserve UICs (RUICs) within the AOR as designated in RHS.

3. **Command View User**.

   a. Application Access. Command View Users are granted access by an Admin or Delegated Admin User within the UIC or in the Echelon II or III command in the ACL.

      1) Command View Users will request access using the guidelines provided separately in this guide.

         a) Access will terminate…

            i) upon transfer or separation from the UIC/RUIC, or

            ii) upon the assigning Admin Access or Delegated Admin User's loss of access, or

            iii) upon access removal by an ACL Admin Access or Delegated Admin User.

   b. OMPF- Command View Application. The Command View role will use the OMPF view application to view, print or download:

      1) OPMF documents in "Non-controlled" Records within their Admin ACL

         a) Officer Command View Users – have access to documents in Officer Field Codes 01, 02, 04 through 16, 18 and 98 as well as Enlisted Field Codes 30 through 43, 45, and 99.

            i) Enlisted, Civilian and Contractor Command View Users – have access to documents in Enlisted Field Codes 30 through 43, 45, and 99.

            ii) If assigned to a designated Personnel Support Detachment, the Command View User will also have access to the OMPFs for the UICs and/or Reserve UICs (RUICs) within the designated AOR.

            iii) If assigned to a Reserve Admin UIC, the Admin Access User will also have access to the OMPFs for the Reserve UICs (RUICs) within the AOR as designated in RHS.

4. **Command-Only View User**.

   a. Application Access. Command-Only View Users are granted access by an Admin or Delegated Admin User within the UIC or in the Echelon II or III command in the ACL.

      1) Command-Only View Users will request access using the guidelines provided separately in this guide.

         a) Access will terminate…

            i) upon transfer or separation from the UIC/RUIC, or

            ii) upon the assigning Admin Access or Delegated Admin User's loss of access, or

            iii) upon access removal by an ACL Admin Access or Delegated Admin User.

   b. OMPF- Command View Application. The Command View role will use the OMPF view application to view, print or download OPMF documents in "Non-controlled" Records within their onboard UIC.

      1) Officer Command-Only View Users – have access to documents in Officer Field Codes 01, 02, 04 through 16, 18 and 98 as well as Enlisted Field Codes 30 through 43, 45, and 99.

      2) Enlisted, Civilian and Contractor Command-Only View Users – have access to documents in Enlisted Field Codes 30 through 43, 45, and 99.

5. **Removal of access by CNPC.** Commands must notify NPC's Records Management/Policy Branch (PERS-313) when authority to access records is to be canceled for any reason and an Admin/ Delegated Access User is not available.

3 The OMPF-Admin Access Application

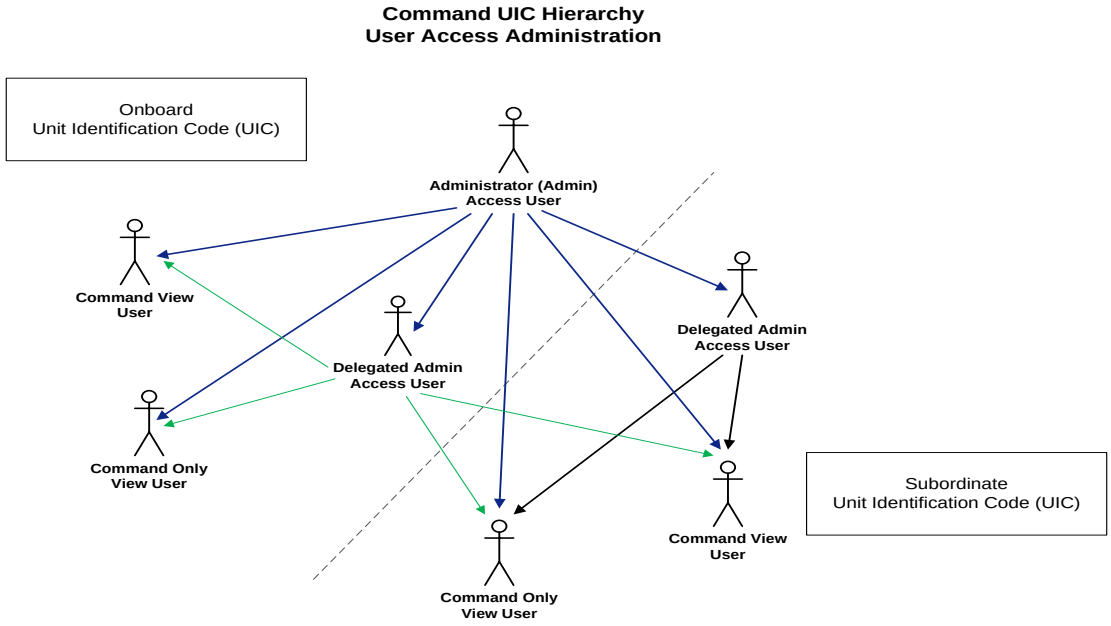
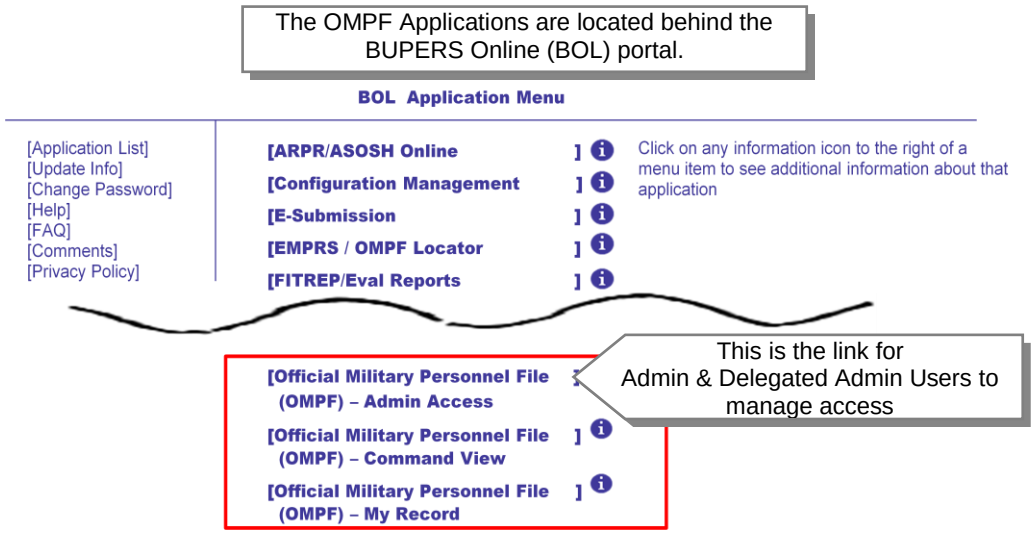


Figure 3-1: Application User Access Administration with UIC Hierarchy

The OMPF-Admin Access application is the command-level administrative tool to manage the roles of Delegated Admin, Command View and Command-Only View for their onboard and subordinate UICs within their Administrative Unit Identification Code (UIC) Access Control List (ACL) hierarchy. The application will also be used to audit OMPF access by the authorized users when necessary.

1. Admin Access Users and Delegated Admin users will access the OMPF-Admin Access application through BUPERS Online (BOL) on the CNPC website at https://www.bol.navy.mil/.

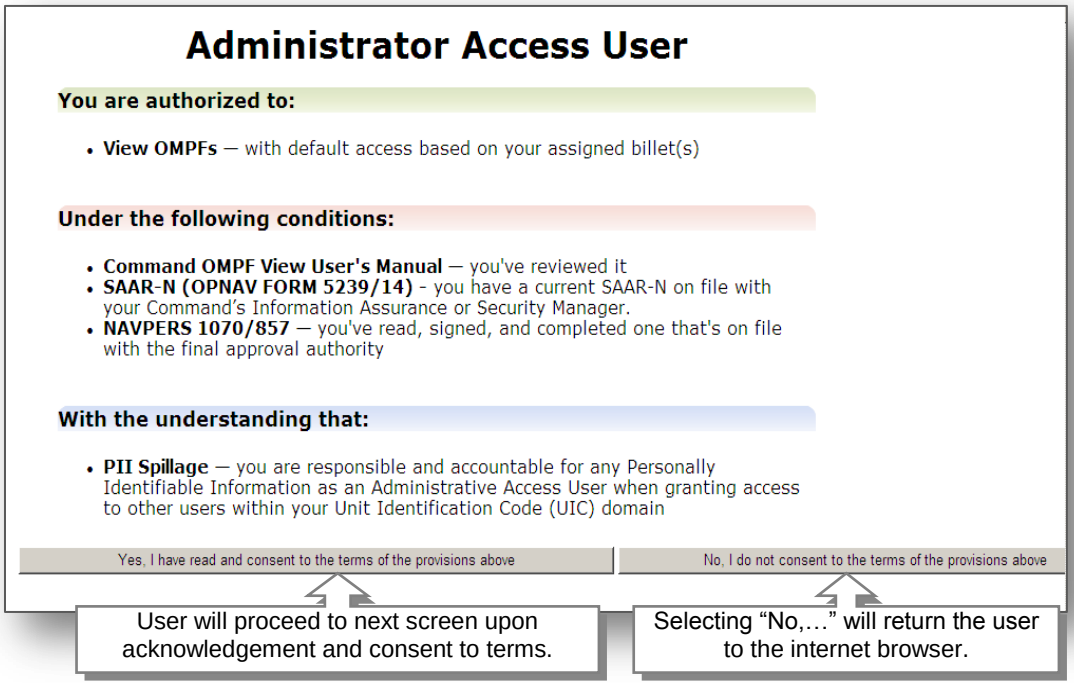


2. On the BOL main menu, select the link for **OMPF-Admin Access** application. If the link is not visible in BOL, your access has not been activated.

   a. If you are attempting to access as an Admin Access User, verify your billet NOBC or DNEC is a listed as a Default User listed in Appendix 6.1.

   b. If you are attempting to access as a Delegated Admin User, *refer to "Access to the OMPF-Administration Access and/or OMPF-Command View Applications" provided in Chapter 5.2 in this guide.*

Upon initial entry into the OMPF-Admin Access application, the Admin Access User must read and acknowledge this screen.



User will proceed to next screen upon acknowledgement and consent to terms.

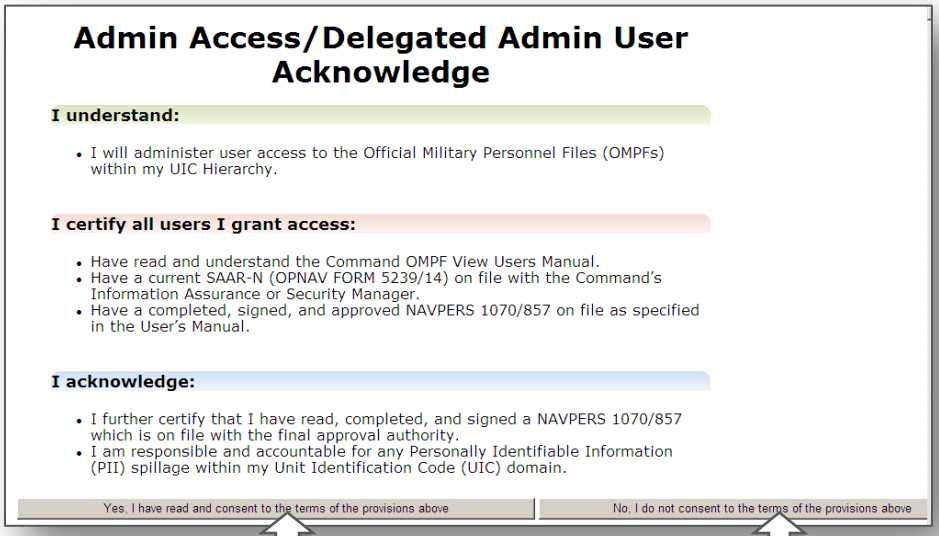
Selecting "No,…" will return the user to the internet browser.

3. The Admin and Delegated Access Users will be presented with the Administrator Access User screen at initial login only. Users are required to read and acknowledge the conditions and terms of accepting access to the OMPF-Admin Access application.

   a. The User must select "**Yes, I have read and consent to the terms of the provisions above**" in order to be navigated to the next screen.

   b. The application will capture the User's consent to the terms and conditions of the application as an audit item for CNPC.

Upon each login, Admin Access and Delegated Admin Users acknowledge responsibility for command and hierarchy.



Selecting "Yes…" will allow the user to enter the application.

Selecting "No,…" will return the user to the BOL main menu.

4. Upon each login, the Admin and Delegated Access Users will be presented with the Admin Access/Delegated Admin User Acknowledgement screen. Although it is very similar to the initial login screen, this emphasizes the terms and conditions for granting access to Delegated Access, Command View or Command-Only View Users.

   a. The User must select "**Yes, I have read and consent to the terms of the provisions above**" in order to be navigated to the application and to the UIC Administration Screen.

5. The UIC Administration Screen will be presented. The User's UIC and subordinate UICs, if any, will be listed in this screen.

This is the UIC Administration Screen.
In this example, the Admin Access or Delegated Access user is assigned to USFF and can select a command to manage user rights.

Select a header to sort…

or use Filters

Return to UIC screen | Search for Records | Return to BOL

UIC	Activity Title	D…	…maining Admins	Assigned Users	Remaining Users
00060	Commander U.S. Fleet Forces Command	1	2	5	31
57012	Commander Naval Air Force, Atlantic	1	1	0	15
03365	ENTERPRISE (CVN 65)	1	15	12	307
09893	EISENHOWER (CVN 69)				
21853	THEODORE ROOSEVELT (				
23170	HARRY S TRUMAN (CVN 75)				
09732	COMCARAIRWING ONE	0	1	0	4
09731	COMCARAIRWING THREE	0	1	0	4
09736	COMCARAIRWING SEVEN	0	1	0	4
09748	COMCARAIRWING EIGHT	0	1	0	4

In this example, the user selects USS ENTERPRISE (CVN 65) to administer rights.

Commands within the User's Access Control List (ACL) are listed.

# of Delegated Admin Users, total Assigned Users and remaining "quotas" are also listed.

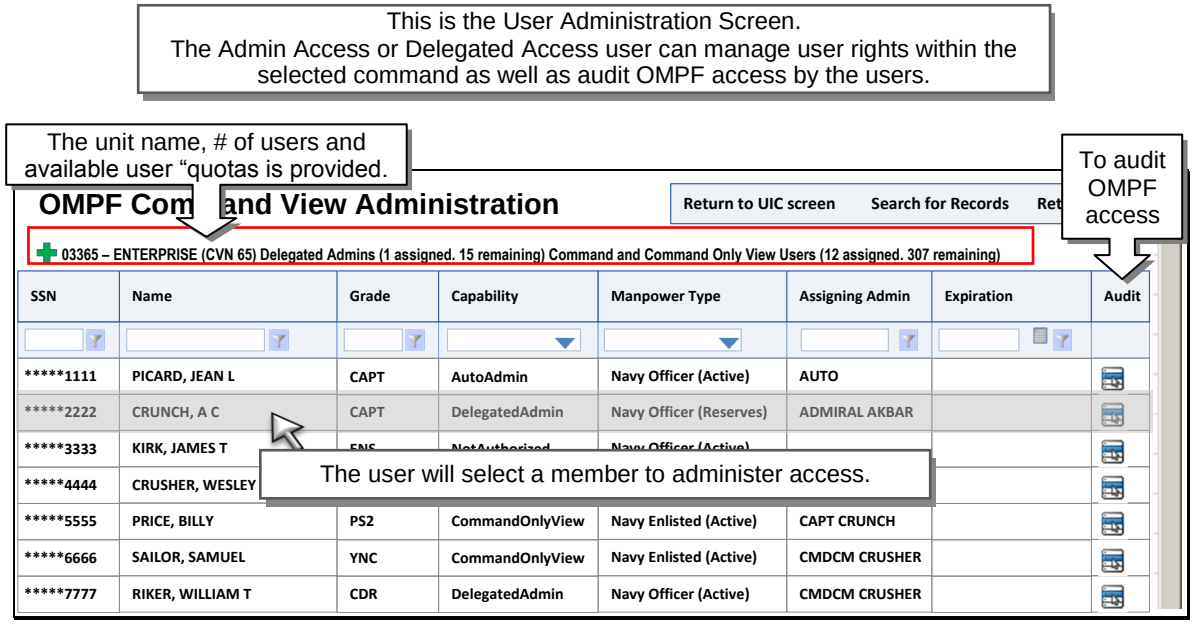
a. Subordinate activities can be quickly located within the listing by selecting a column header to sort in ascending or descending order, or by filtering on part or all of the UIC or Activity Title.

1) For Admin and Delegated Admin Users in Reserve Admin UICs, the Admin UIC and supported Reserve UICs (RUICs) will be listed.

2) For PSD Delegated Admin Users, once your access has been granted by CNPC, you will be presented your onboard UIC.

b. The user will then "select" the UIC to manage access to and the User will be presented the User Administration screen.

6. The User Administration Screen will be presented.



SSN	Name	Grade	Capability	Manpower Type	Assigning Admin	Expiration	Audit
*****1111	PICARD, JEAN L	CAPT	AutoAdmin	Navy Officer (Active)	AUTO		
*****2222	CRUNCH, A C	CAPT	DelegatedAdmin	Navy Officer (Reserves)	ADMIRAL AKBAR		
*****3333	KIRK, JAMES T						
*****4444	CRUSHER, WESLEY						
*****5555	PRICE, BILLY	PS2	CommandOnlyView	Navy Enlisted (Active)	CAPT CRUNCH		
*****6666	SAILOR, SAMUEL	YNC	CommandOnlyView	Navy Enlisted (Active)	CMDCM CRUSHER		
*****7777	RIKER, WILLIAM T	CDR	DelegatedAdmin	Navy Officer (Active)	CMDCM CRUSHER		

Note: All User names and partially-masked SSN's displayed in this User guide are fictitious.

a. Users can sort each of the columns by selecting a header, or filter each field to limit list of UIC members displayed:

1) **SSN** – User can filter SSNs by entering part of the last 4 digits of the member's SSN and using "EndsWith" or "Contains".

2) **Name** – User can filter on part of the member's name.

3) **Grade** – User can filter by using either pay grade (e.g. Greaterthan E5 will give all military E6 & above), or the Grade abbreviation (e.g. EqualTo CAPT). *For Warrant Officers, you must use the Grade abbreviation (e.g. Contains CWO) and not the pay grade (e.g. EqualTo W2).*

4) **Capability** – Use dropdown menu to select from "**AutoAdmin** (Admin Access User), "**Delegated Admin**, "**Command View**", "**CommandOnlyView**" and "**NotAuthorized**" (does not have user rights).

5) **Manpower Type** – Use dropdown menu to limit list to a specific manpower community (e.g. Navy Officer (Active)).

6) **Assigning Admin** – Sort or filter by who authorized access

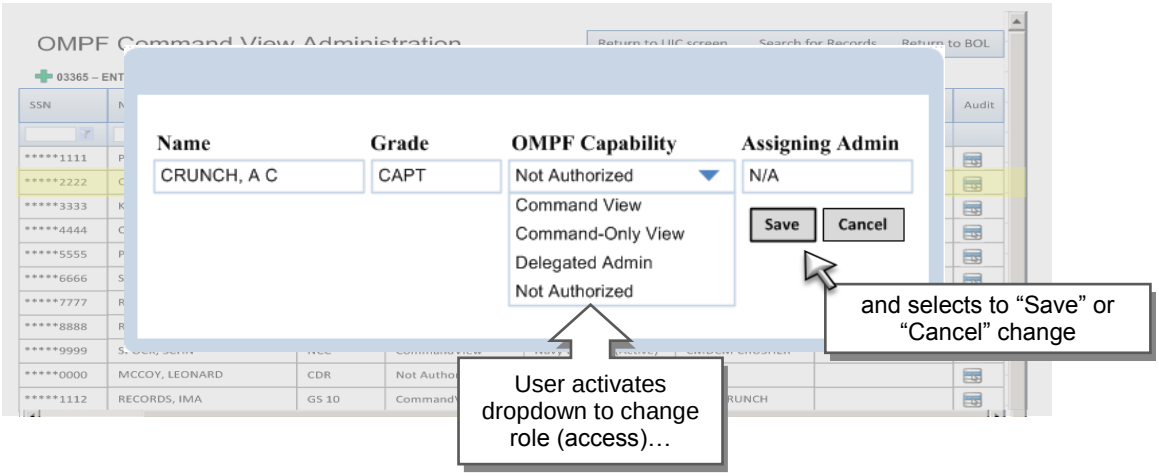
(1) Name of Admin Access or Delegated Admin User who assigned the access, or

(2) Name of the final approving authority annotated on the NAVPERS 1070/857, when access is granted by CNPC (PERS-31). *Refer to Chapters 5.1 and 5.2.*

7) **Expiration** – Sort, or filter (by using the calendar icon) on authorized users who were given an expiration date by CNPC.

8) *The Audit option is covered in paragraph 8 in this section.*

7. Managing Access - As indicated in the User Administration screen, the User will "select" the member to manage access for.



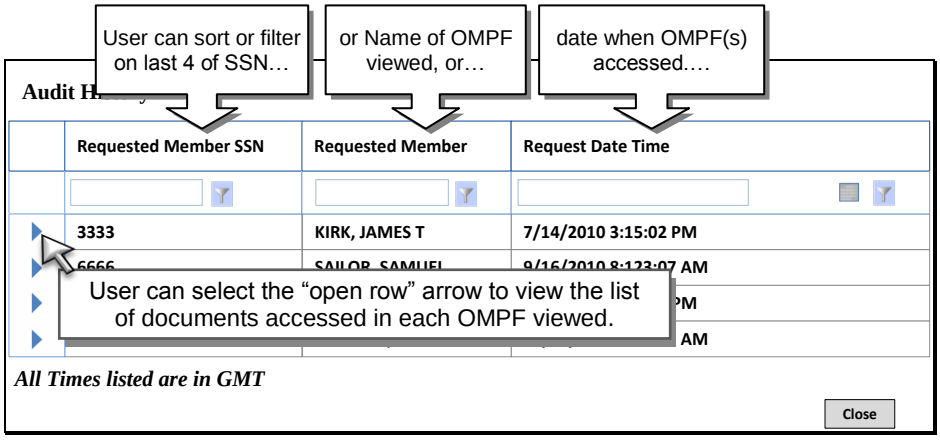
Note: All User names and partially-masked SSN's displayed in this User guide are fictitious.

a. A pop-up screen will be presented.

b. The User will use the OMPF Capability dropdown menu to select the appropriate access level for the selected member. *PSD Delegated Admin Users will not be presented with the "**Delegated Admin**" option as this role must be granted by CNPC.*

c. Upon saving selection, the User will be navigated back to the User Administration Screen with the number of authorized Users and remaining "quotas" adjusted accordingly.

8. Auditing OMPF Access – As indicated in the User Administration Screen, the User can select the "Audit" button on a member row (*refer to 6.a.*) to view what OMPFs the particular User has accessed.



Note: All User names and partially-masked SSN's displayed in this User guide are fictitious.

a. A pop-up Audit History screen will be presented.

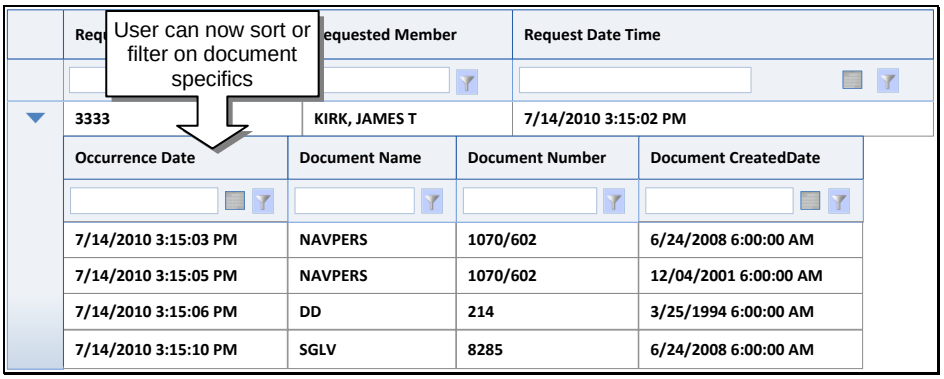
b. Users can sort each of the columns by selecting a header, or filter each field to limit list of members whose OMPFs were viewed:

1) **SSN** – User can filter SSNs by entering part of the last 4 digits of the member's SSN and using "EndsWith" or "Contains".

2) **Name** – User can filter on part of the member's name.

3) **Requested Date Time** – User can sort, or filter (by using the calendar icon) on a particular date and time the OMPFs were viewed. *Times listed are Greenwich Mean Time (GMT).*

c. The User can select the open row arrows next to the OMPF viewed and will be presented the list of documents accessed within the OMPF.



Note: All User names and partially-masked SSN's displayed in this User guide are fictitious.

d. Users can sort each of the columns in the document list by selecting a header, or filter each field:

1) **Occurrence Date** – Sort or filter (by using the calendar icon) on a particular date and time the documents within the OMPF were viewed. *Times listed are Greenwich Mean Time (GMT).*

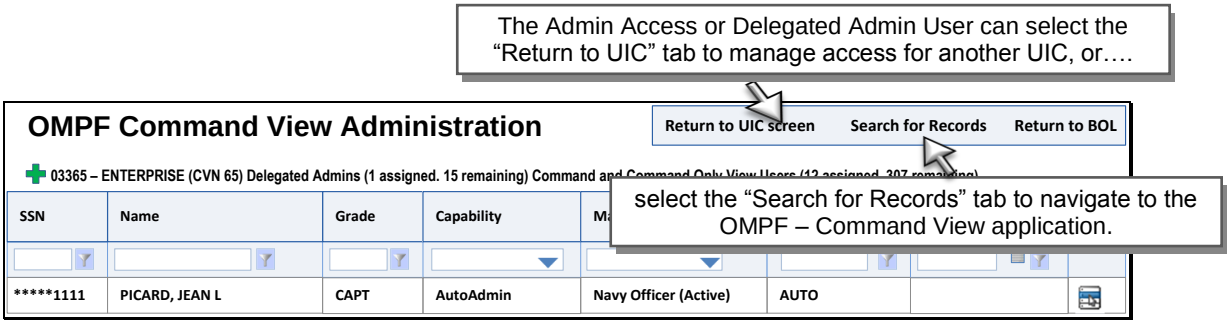
2) **Document Name** - Sort or filter by type of form.

3) **Document Number** – Sort or filter by form number

4) **Document CreatedDate** – Sort or filter (by using the calendar icon) by date the OMPF document was created.

e. The User will select the "Close" button to return to the User Administration Screen.

9. Selecting to Search for an OMPF.



a. From the Unit and the User Administration Screens, the Admin or Delegated Admin User can select to "**Search for a Record**".

b. Upon selecting the "**Search for a Record**" tab, the User will be presented the OMPF-Command View application Protection of Record Information Screen and will bypass the link on the BOL main menu.

c. *Upon acknowledging the terms and conditions, the User will be able to navigate through the OMPF-Command View application as outlined in Chapter 4 of this user guide.*

4 The OMPF- Command View Application

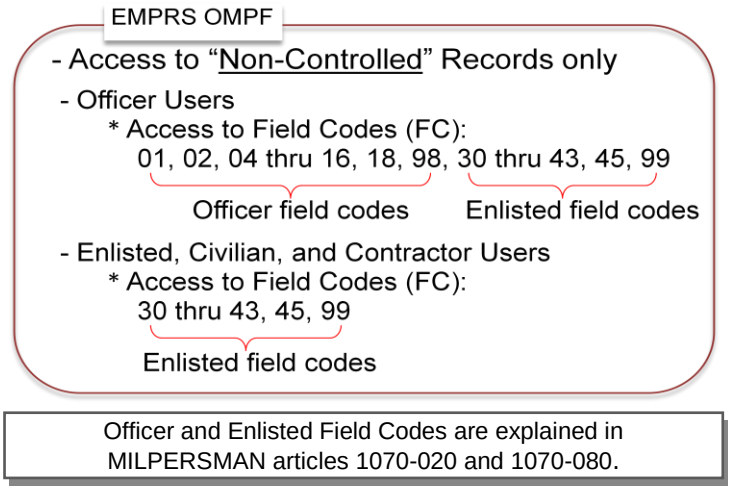


Figure 4-1: EMPRS OMPF Access

The OMPF-Command View Application provides authorized Users a web-based interface to Officer and Enlisted official record information that is not available in other official data sources and is only contained in the Official Military Personnel File (OMPF).

1. Access will be to "non-controlled" records only.

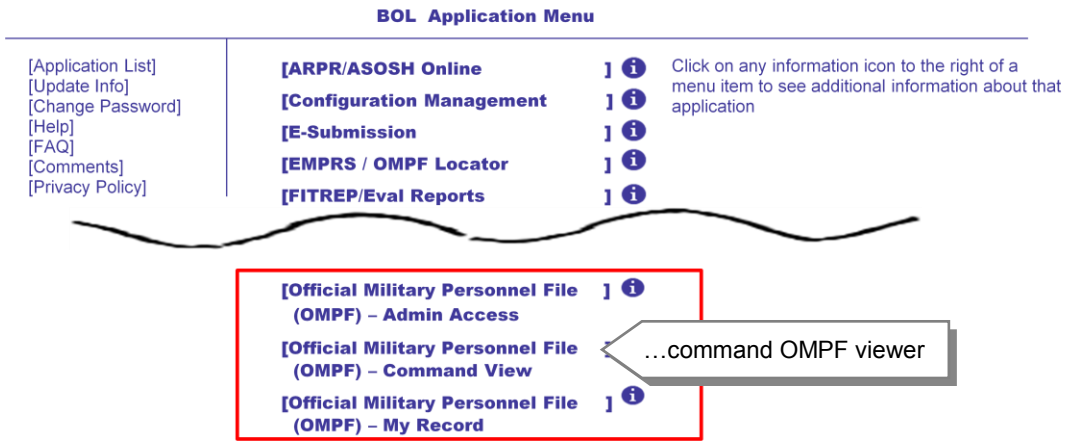
    a. Admin Access, Delegated Admin and Command View Users will have access to OMPFs in their onboard UIC and subordinate UICs within their Admin ACL.

    b. Command-Only View Users will have access to OMPFs in their onboard UIC.

    c. Officer Users will have access to Officer and Enlisted documents contained in the field codes listed in Figure 4-1. *Refer to the MILPERSMAN articles listed in Figure 4-1 as well as Appendices 6.3 and 6.4 of this guide for more field code information.*

    d. Enlisted, Civilian and Contractor Users will have access to Enlisted documents contained in the field codes listed in Figure 4-1.

2. Users will access the OMPF-Command View application through BUPERS Online (BOL) on the CNPC website at https://www.bol.navy.mil/. *Admin and Delegated Admin Users have the ability to access the OMPF-Command View application from the OMPF-Admin Access application by selecting "Search for Records".*

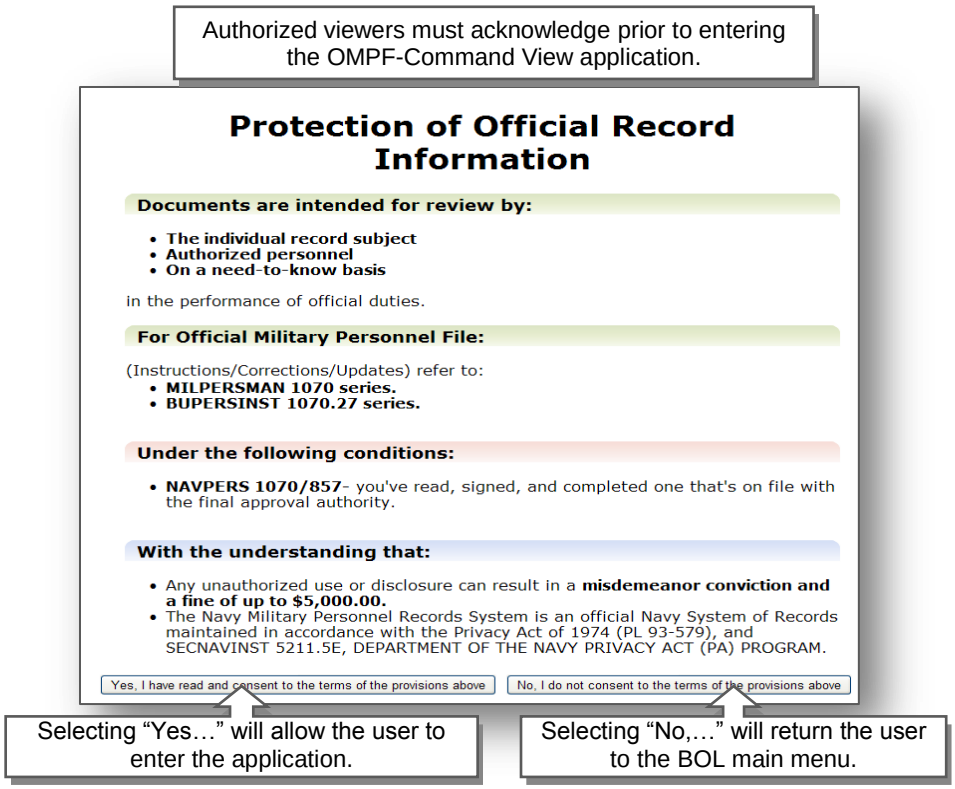


3. On the BOL main menu, select the link for **OMPF-Command View** application. If the link is not visible in BOL, your access has not been activated.

   a. If you are attempting to access as an Admin Access User, verify your billet NOBC or DNEC is a listed as a Default User listed in Appendix 6.1.

   b. If you are attempting to access as a Delegated Admin, Command View or Command-Only View User, *refer to "Access to the OMPF-Administration Access and/or OMPF-Command View Applications" provided separately in this guide*.

4. Upon each login, all authorized Users will be presented with the Protection of Record Information Acknowledgement screen. This screen emphasizes the terms and conditions for granting access to the "**For Official Use Only**" information contained in the OMPFs.

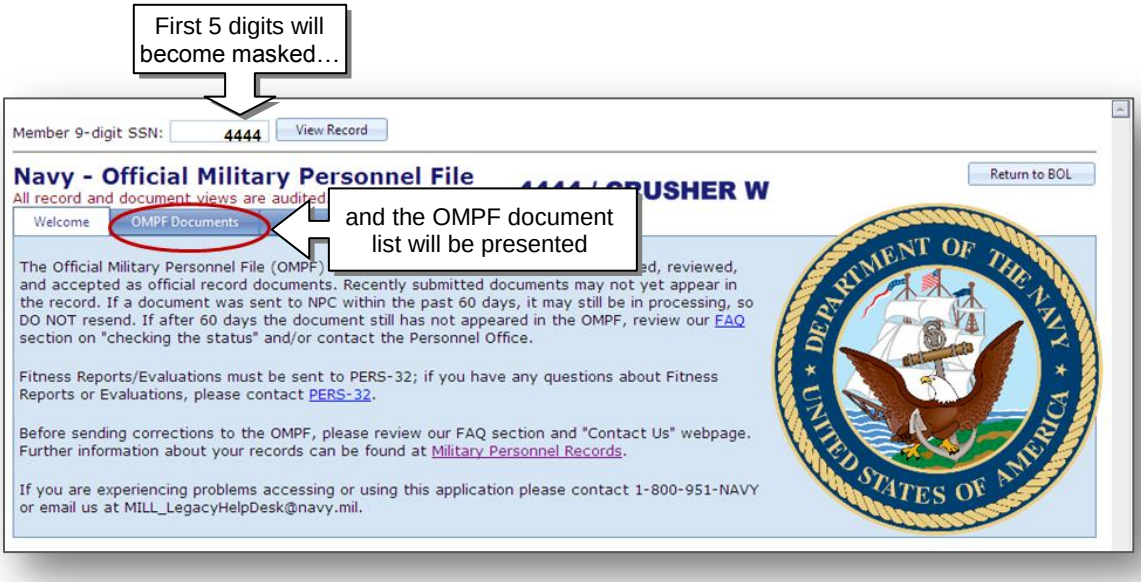


a. The User must select "**Yes, I have read and consent to the terms of the provisions above**" in order to be navigated to the application's Welcome Screen.

5. The OMPF-Command View Welcome Screen will be presented.

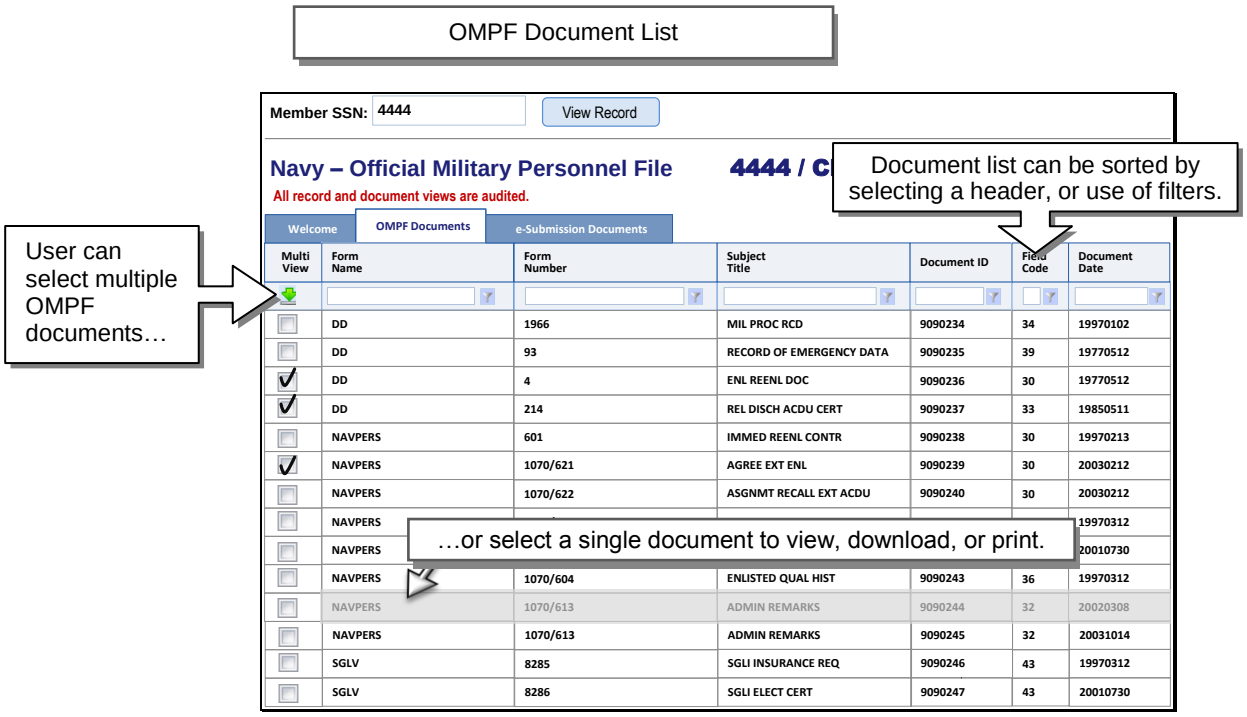
6. The Welcome screen provides the User with additional information resources pertaining to the OMPFs.

7. The User must enter a 9-digit SSN to search for a record and then select "**View Record**".



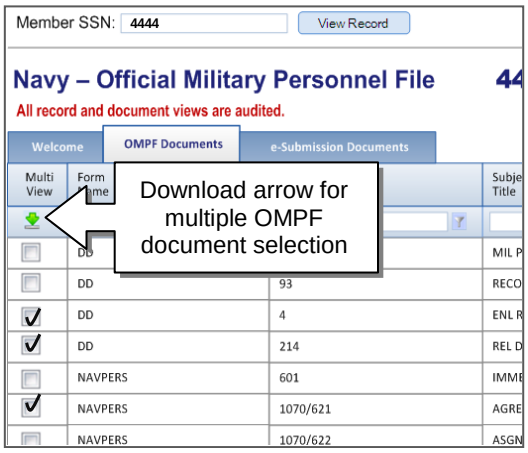
Note: All User names and partially-masked SSN's displayed in this User guide are fictitious.

8. The first 5 digits of the SSN will become masked and the OMPF Document List will be presented. *The error message "**No viewable OMPF found (XXXXXXXXX)**" will be presented if the User is not authorized access to the requested OMPF.*



9. The OMPF Document List. OMPF Documents can be quickly located within the listing by selecting a header to sort in ascending or descending order, or by filtering on all or part of the document identifiers:
   a. **Form Name** - Sort or filter by type of form.
   b. **Form Number** – Sort or filter by form number
   c. **Subject Title** – Sort or filter by the form subject title
   d. *Document ID – Used internally by CNPC*
   e. **Field Code** – Sort or filter by OMPF field codes.
   f. **Document Date** – Sort or filter by the date of the document.
10. Single document View, Print or Download.
   a. User will "select" the document by "clicking" anywhere on the document row.
   b. Adobe Reader will be invoked.
      1) The document will be presented in Adobe Reader.
      2) All documents will contain the official record watermark.
      3) The User can select to print, save (download) or close the single document from the Adobe Reader File menu. *Users are cautioned NOT to keep repositories of downloaded or printed documents as these types of files are not covered under a Privacy Act System of Records Notice (PA SORN).*

11. Multiple document View, Print or Download.

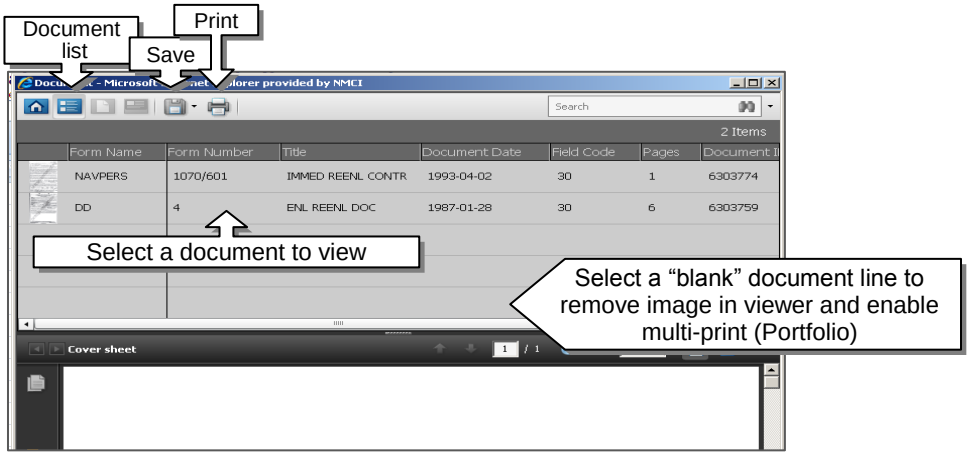


a. The User will "check" the boxes in the Multi View column to view, print or download the selected documents.

b. The User will select the download arrow in the Multi View column.

c. Adobe Reader will be invoked.

d. A PDF Portfolio document list will be presented in Adobe Reader.



1) <u>To view a document</u>.

   a) The User will select the document row and the image will be presented in the image view box.

   b) All documents will contain the official record watermark.

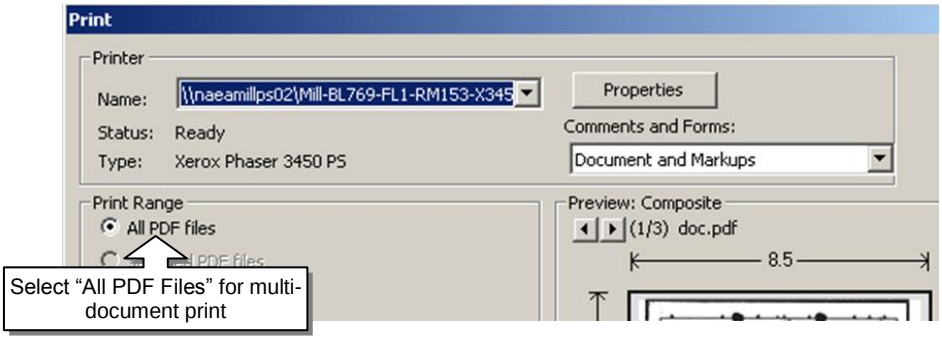
2) <u>To save (download) or close the PDF portfolio</u>. The User will select "**Save**" or "**Close**" from the Adobe Reader **File** menu. *Users are cautioned NOT to keep repositories of downloaded or printed documents as these types of files are not covered under a Privacy Act System of Records Notice (PA SORN).*

3) <u>To print a PDF portfolio</u>.

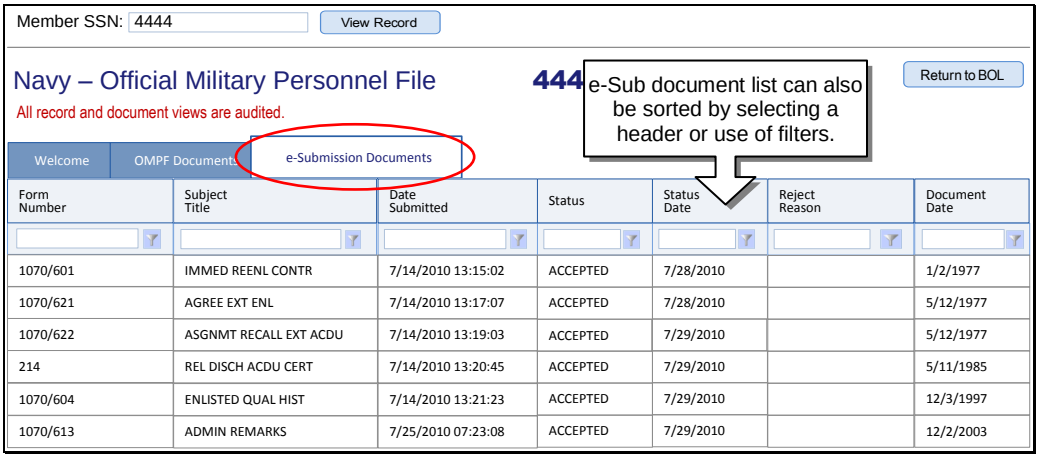
   a) User will select a blank document row.

   b) User will select the "**Print**" icon.

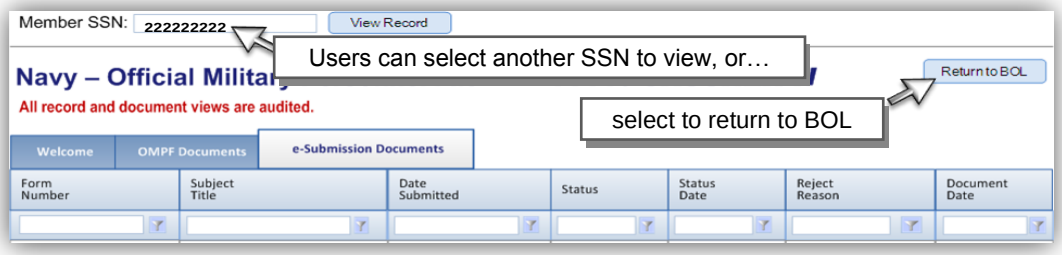
   c) User will select the "**All PDF files**" radial button and select "**Print**".



12. Users can also view the status of documents submitted to the OMPF through the e-Submission application by selecting the "**e-Submission**" tab.



13. <u>e-Submission Document Status</u>. Users can filter or sort the e-Sub list by selecting a header to sort in ascending or descending order, or by filtering on all or part of the document identifiers:
    a) **Form Number** – Sort or filter by form number
    b) **Subject Title** – Sort or filter by the form subject title
    c) **Date Submitted** – Sort or filter by the date and time document was submitted by the e-Sub User
    d) **Status** – Sort or filter by the status of the document (Accepted, Rejected, Pending or Research). *Refer to the Enlisted Field Service Record Closeout Guide located on the CNPC website for more status information.*
    e) **Status Date** – Sort or filter by the date the document status was established
    f) **Reject Reason** – Sort or filter by the rejection reason, if the document was rejected.
    g) **Document Date** – Sort or filter by the date of the document.
14. Users can select to view another OMPF, or return to the BOL main menu.



5 Supporting Processes

5.1 Submission of the System Authorization Access Request-Navy Form (SAAR-N)

Navy policy requires all users accessing Navy Information Technology (IT) resources to have a completed System Authorization Access Request-Navy form (SAAR-N) (OPNAV 5239/14 – July 2008) on file with the authorizing agency. The SAAR-N form is available to download at the Naval Forms website at https://navalforms.daps.dla.mil/web/public/home.

OMPF-Administrator Access and/or OMPF-Command View User Role granted at the local level.

Prior to accessing the OMPF-Admin Access and/or the OMPF-Command View applications, Admin Access Users and all other users granted access at the local or upper Echelon level, will have on file with the command's Information Assurance or Security Manager:

- An updated SAAR-N, and
- A completed Request for Access to Electronic Military Personnel Records System (EMPRS) (NAVPERS 1070/857). *Directions for completing the NAVPERS 1070/857 are provided in Chapter 5.2 of this guide.*

OMPF-Administrator Access and/or OMPF-Command View User Role granted by CNPC.

A completed SAAR-N and NAVPERS 1070/857 must be forwarded to CNPC for:

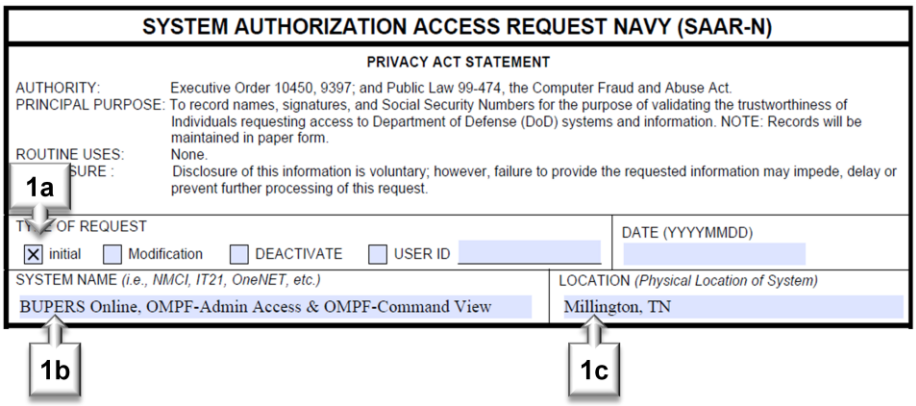
- Users requesting access as a PSD Delegated Admin User,
- Users who do not have a current BUPERS Online (BOL) account, or
- Users who do not have an Admin Access User or Delegated Admin User in their ACL hierarchy to grant access.

SAAR-N completion requirements for access granted by CNPC.

The user must complete the SAAR-N as outlined in this chapter, and forward to CNPC along with the completed NAVPERS 1070/857.

All blocks must be completed as outlined on page 4 of the SAAR-N form in addition to the amplifying instructions provided herein which are specific for access to BOL, and applications residing on BOL.

1. Top Section:



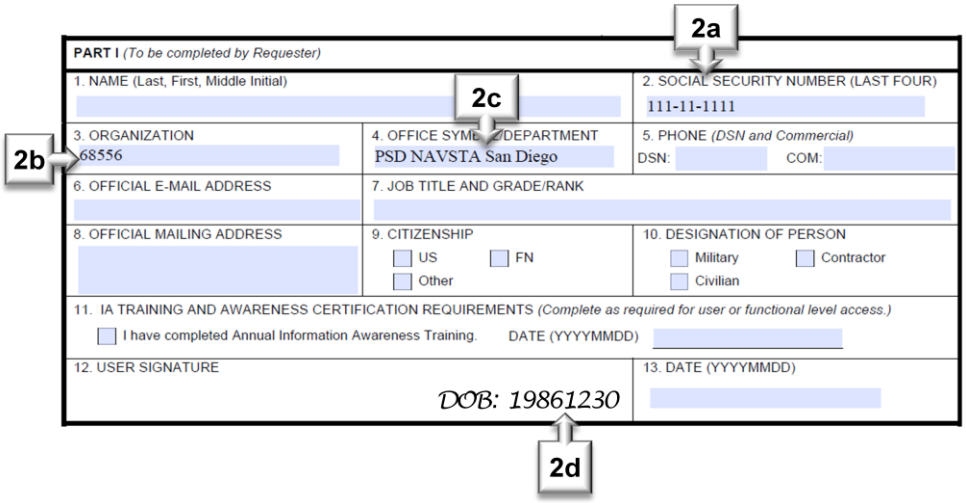
Refer to PG. 4 of the SAAR-N for block-by-block completion requirements in addition to these amplifying instructions.

ALL blocks must be complete unless otherwise specified.

a. **Type of Request**. Check "Initial".
b. **System Name**.
   (1) User does not have BOL access…
      (a) Type "**BUPERS Online**" and…
         - "**OMPF-Admin Access & OMPF-Command View**" for PSD Delegated Admin or Delegated Admin role, or…
         - "**OMPF-Command View**" for Command View and Command-Only View role.
   (2) User does have BOL access…
      (a) Type "**OMPF-Admin Access & OMPF-Command View**" for PSD Delegated Admin or Delegated Admin role, or…
      (b) Type "**OMPF-Command View**" for Command View or Command-Only View role.

c. **Location**. Type **Millington, TN** for physical location of system.

2. PART I

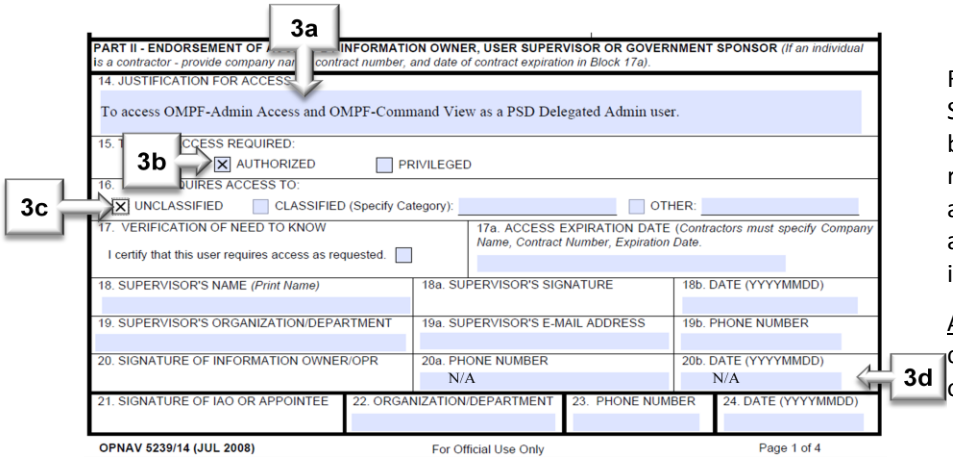


Refer to PG. 4 of the SAAR-N for block-by-block completion requirements in addition to these amplifying instructions.

ALL blocks must be complete unless otherwise specified.

a. **Social Security Number**. All nine (9) digits of the SSN must be provided. The request cannot be processed with a truncated SSN.
b. **Organization**. Fill in the assigned Unit Identification Code (UIC).
c. **Office Symbol/Department**. Type the activity name.
d. **User Signature**. Date of birth should be included in block 12 along with the user signature.

3. PART II



Refer to PG. 4 of the SAAR-N for block-by-block completion requirements in addition to these amplifying instructions.

ALL blocks must be complete unless otherwise specified.

a. **Justification for Access**.

(1) For PSD Delegated Admin (or Delegated Admin) user, type…

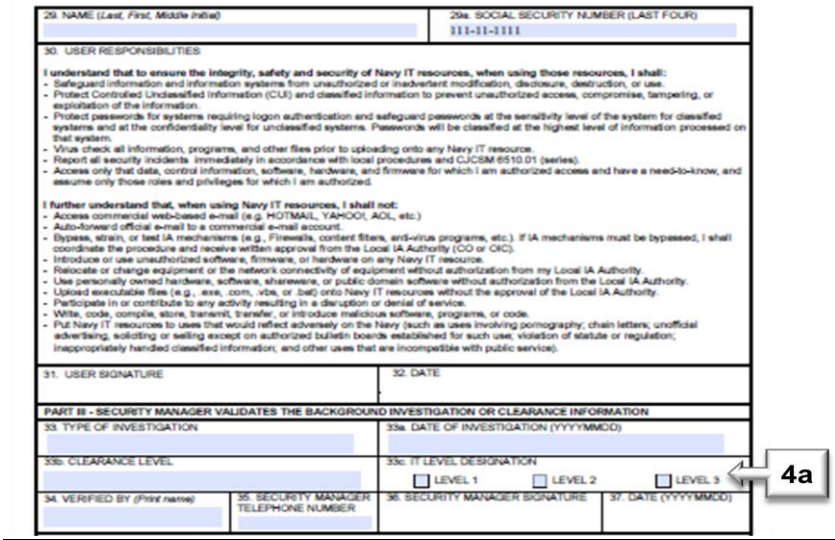
To access OMPF-Admin Access and OMPF-Command View as a PSD Delegated Admin (or **Delegated Admin**) **user**

(2) For Command View or Command-Only View user, type

"To access OMPF-Command View as a Command View (or **Command-Only**) **user**

b. **Type of Access Required**. Check **Authorized.**
c. **User Requires Access to.** Check **Unclassified.**
d. **Signature of Information Owner/OPR**. Blocks 20, 20a and 20b should remain blank or marked **N/A** unless member is assigned to NPC. If member is assigned to NPC, member's IAM will complete this block.

4. PART III**.** This part must be completed by the command's security manager.

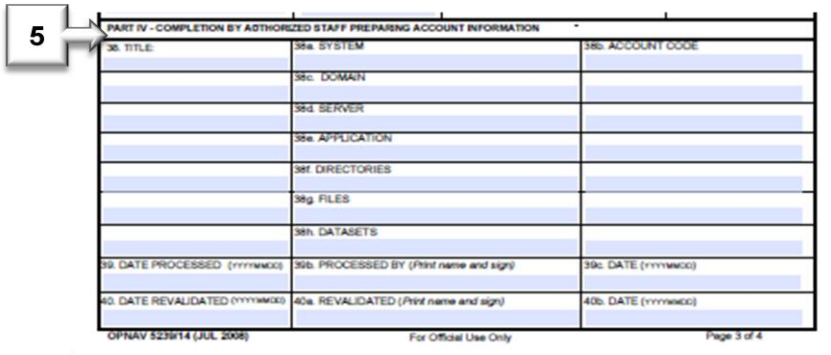


Refer to PG. 4 of the SAAR-N for block-by-block completion requirements in addition to these amplifying instructions.

ALL blocks must be complete unless otherwise specified.

a. **IT Level Designation**. Check one of the Investigation Type (IT) Levels in block 33c. Although a security clearance is not required for access to BOL, an active background investigation is.

5. PART IV. Leave blank. This will be completed by CNPC staff.



6. Submitting the completed SAAR-N

   a. Verify Parts I, II and III are completely filled in and contain all appropriate signatures. Incomplete requests will be denied.

   b. Fax - the completed and signed form can be faxed to 901-874-2722, or…

   c. Email - the completed and signed form can be emailed to **diane.mcdaniel.ctr@navy.mil**.

      (1) If sent via email, the email must be encrypted and signed with a digital signature in order to protect the personal information contained in the form.

   d. The originals of both forms will be retained by your command Information Assurance Manager or Security Manager.

7. BOL access. Requests should be processed at CNPC within 72-96 hours from receipt.

All civilian, contractor and other non-Navy employee accounts are set to expire in a 90-day cycle. If there is no activity during that 90-day period, the account will expire. If your account does expire, updated paperwork will have to be submitted.

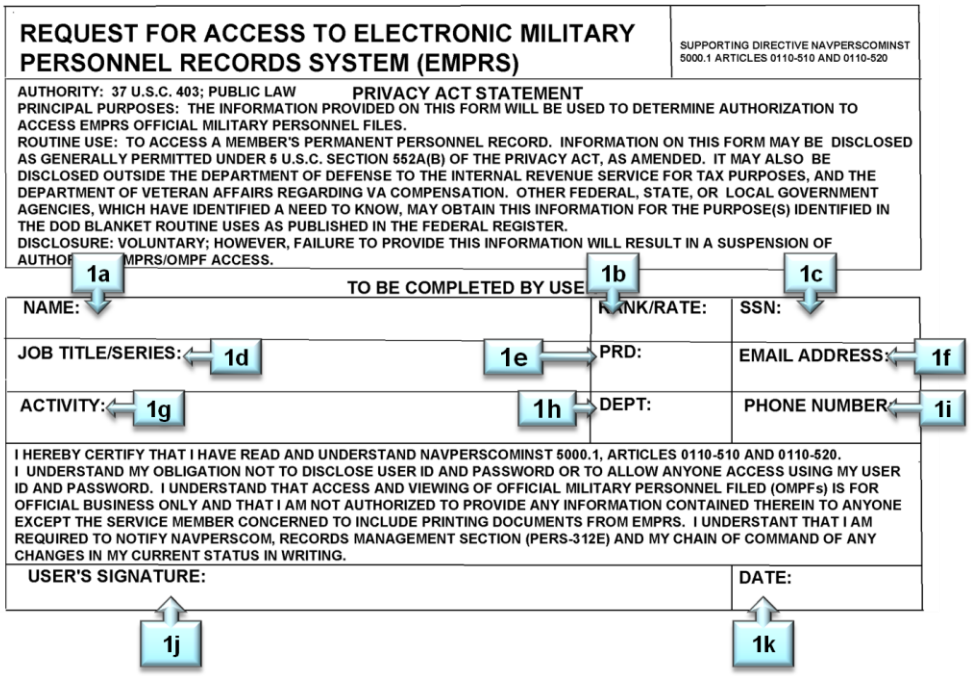
5.2 Access to the OMPF-Administration Access and/or OMPF-Command View Applications

Requesting a User Role in the OMPF-Admin Access and/or OMPF-Command View Applications

The user must first complete and submit a NAVPERS 1070/857, Request for Access to Electronic Military Personnel Records System (EMPRS), which is available for download at http://www.npc.navy.mil/ReferenceLibrary/Forms/NAVPERS/.

The process for completing the EMPRS access request form is as follows:

1. **Section 1** of the form is titled "To be completed by user" and identifies the trusted source and assigned activity.


REQUEST FOR ACCESS TO ELECTRONIC MILITARY PERSONNEL RECORDS SYSTEM (EMPRS)

SUPPORTING DIRECTIVE NAVPERSCOMINST 5000.1 ARTICLES 0110-510 AND 0110-520

AUTHORITY: 37 U.S.C. 403; PUBLIC LAW

PRIVACY ACT STATEMENT

PRINCIPAL PURPOSES: THE INFORMATION PROVIDED ON THIS FORM WILL BE USED TO DETERMINE AUTHORIZATION TO ACCESS EMPRS OFFICIAL MILITARY PERSONNEL FILES.

ROUTINE USE: TO ACCESS A MEMBER'S PERMANENT PERSONNEL RECORD. INFORMATION ON THIS FORM MAY BE DISCLOSED AS GENERALLY PERMITTED UNDER 5 U.S.C. SECTION 552A(B) OF THE PRIVACY ACT, AS AMENDED. IT MAY ALSO BE DISCLOSED OUTSIDE THE DEPARTMENT OF DEFENSE TO THE INTERNAL REVENUE SERVICE FOR TAX PURPOSES, AND THE DEPARTMENT OF VETERAN AFFAIRS REGARDING VA COMPENSATION. OTHER FEDERAL, STATE, OR LOCAL GOVERNMENT AGENCIES, WHICH HAVE IDENTIFIED A NEED TO KNOW, MAY OBTAIN THIS INFORMATION FOR THE PURPOSE(S) IDENTIFIED IN THE DOD BLANKET ROUTINE USES AS PUBLISHED IN THE FEDERAL REGISTER.

DISCLOSURE: VOLUNTARY; HOWEVER, FAILURE TO PROVIDE THIS INFORMATION WILL RESULT IN A SUSPENSION OF AUTHO MPRS/OMPF ACCESS.

1a 1b 1c

TO BE COMPLETED BY USE

NAME: | NK/RATE: | SSN:

JOB TITLE/SERIES: 1d | 1e PRD: | EMAIL ADDRESS: 1f

ACTIVITY: 1g | 1h DEPT: | PHONE NUMBER 1i

I HEREBY CERTIFY THAT I HAVE READ AND UNDERSTAND NAVPERSCOMINST 5000.1, ARTICLES 0110-510 AND 0110-520. I UNDERSTAND MY OBLIGATION NOT TO DISCLOSE USER ID AND PASSWORD OR TO ALLOW ANYONE ACCESS USING MY USER ID AND PASSWORD. I UNDERSTAND THAT ACCESS AND VIEWING OF OFFICIAL MILITARY PERSONNEL FILED (OMPFs) IS FOR OFFICIAL BUSINESS ONLY AND THAT I AM NOT AUTHORIZED TO PROVIDE ANY INFORMATION CONTAINED THEREIN TO ANYONE EXCEPT THE SERVICE MEMBER CONCERNED TO INCLUDE PRINTING DOCUMENTS FROM EMPRS. I UNDERSTANT THAT I AM REQUIRED TO NOTIFY NAVPERSCOM, RECORDS MANAGEMENT SECTION (PERS-312E) AND MY CHAIN OF COMMAND OF ANY CHANGES IN MY CURRENT STATUS IN WRITING.

USER'S SIGNATURE: | DATE:

1j 1k

a. **Name**. Fill in last name, first name and middle initial (e.g. Smith, John J.)

b. **Rank/Rate**.

(1) If military, list actual Rate or Rank (e.g. PS1 or LT)

(2) If government civilian, annotate "CIV".

(3) If contractor, annotate "CONT".

c. **SSN**. Complete all 9 digits of your social security number. The request cannot be processed with a truncated SSN.

d. **Job Title/Series**. List functional title (e.g. personnel clerk)

e. **PRD**.

(1) If military, month and year you are projected to transfer from current activity

(2) If government civilian or contractor, annotate "N/A"

f. **Email address**. Official email address

g. **Activity**. Name of command and assigned Unit Identification Code (UIC) (e.g. NOSC Millington/61962)

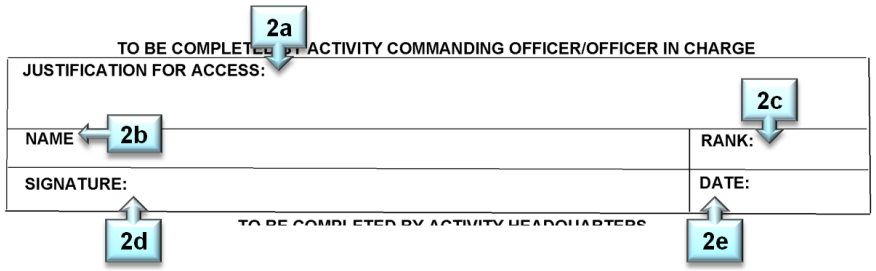
h. **Dept**. Command department assigned

i. **Phone number**. List commercial phone number

j. **User's signature**. This signature certifies that you have read and understand the EMPRS access conditions listed above the signature line as well as certifying your information contained on the request form.

k. **Date**. Signature date

2. **Section 2** of the form is titled "To be completed by Activity Commanding Officer/ Officer in Charge". This section must be completed by Commanding Officer (CO), Officer in Charge (OIC), or Director of a designated personnel activity. COs, OICs and Directors can designate "by direction" signature authority for this form.



a. **Justification for Access**. Comments should include the User Role (**i.e. Delegated Admin, PSD Delegated Admin, Command View and Command-Only View**) to support the level of access and authority to view the records.

b. **Name**. Complete name as outlined in the signature authority designation and title or position. If signing by direction include the wording "By Dir".

c. **Rank/Rate**.

(1) If military, list actual Rate or Rank (e.g. PS1 or LT)

(2) If government civilian, annotate "CIV"

d. **Signature.** This signature certifies that the trusted agent is authorized access to view OMPFs as well as certifying the information contained on the request form.

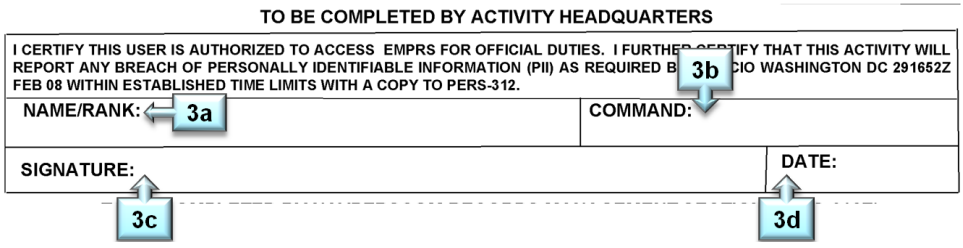
e. **Date**. Signature date

3. **Section 3** of the form is titled "To be completed by Activity Headquarters".

a. For User access to be granted access by an Admin or Delegated Admin User assigned in the command. This may remain blank as your chain of command has certified access in the previous section.

b. For User access to be granted access by an Admin or Delegated Admin User assigned in your Echelon II or III. This section must be completed by your activity's Immediate Superior in Command (ISIC).

c. For User access to be granted by CNPC. This section must be completed by your activity's Immediate Superior in Command (ISIC).



a. **Name/Rank**. Complete name as outlined in the signature authority designation, title or position and rank or rate.

(1) If military, list actual Rate or Rank (e.g. PS1 or LT)

(2) If civilian, annotate "CIV"

b. **Command**. Name of command and assigned Unit Identification Code (UIC) (e.g. NPPSC/40389)

c. **Signature**. This signature certifies that the trusted agent is authorized the requested OMPF User Role within the appropriate application as well as certifying the information contained on the request form.

d. **Date**. Signature date

4. **Section 4** of the form is used by Navy Personnel Command for those that must be forwarded to CNPC.

Retention of the Completed NAVPERS 1070/857

1. For Access to be granted at the command level. The completed form should be retained by your command Information Assurance Manager or Security Manager along with your current System Authorization Access Request-Navy form (SAAR-N) (OPNAV 5239/14 – July 2008). *Refer to Chapter 5.1 of this guide.*

2. For User access to be granted by an Admin or Delegated Admin User assigned in your Echelon II or III. Once approved and access granted is granted at the senior command, the completed NAVPERS form should be returned to your command to be retained by the Information Assurance Manager or Security Manager with your current System Authorization Access Request-Navy form (SAAR-N) (OPNAV 5239/14 – July 2008).

3. For User access to be granted by CNPC. The completed NAVPERS form and updated SAAR-N must be sent to Navy Personnel Command's Records Support Division for review and adjudication via fax or email as outlined below. The originals of both forms are to be retained by your command Information Assurance Manager or Security Manager. *Directions for completing the SAAR-N when required to be sent in to CNPC are provided in Chapter 5.1 of this guide.*

    a. Verify all parts of both the SAAR-N and NAVPERS 1070/857 are completely filled in as specified in this guide and contain all appropriate signatures. Incomplete requests will be denied.

    b. Fax - the completed and signed form can be faxed to 901-874-2722, or…

    c. Email - the completed and signed form can be emailed to **diane.mcdaniel.ctr@navy.mil**.

        (1) If sent via email, the email must be encrypted and signed with a digital signature in order to protect the personal information contained in the form.

    d. If access is granted, the **OMPF-Admin Access** and/or **OMPF-Command View** link(s) will be listed on the BOL Application Menu.

5.3 Updating the Administrative Unit Identification Code (UIC) Hierarchy

1. **Administrative Fleet and Shore Unit Identification Code (UIC) Hierarchy**

Users are advised to follow the procedures outlined in The Navy Organization Change Manual (OPNAVINST 5400.44), October 2008 for requesting changes to the Administrative Fleet and Shore Chain of Command structure.

OPNAVINST 5400.44 outlines the formal organization change process is necessary to "manage the force structure and maintain currency of the administrative organizations and Echelon status in the Standard Navy Distribution List (SNDL) (OPNAVNOTE 5400)". This serves the purpose of providing a formal and current record of the Navy's administrative command (Echelon) structure.

The guide further states the "SNDL is a complete listing of all SECNAV and CNO approved commands and detachments of the operating forces and the shore establishment of the Department of the Navy and the administrative chains of command of the operating forces and shore establishment."

2. **Reserve Administrative Unit Identification Code (UIC)/Supported Reserve Unit Identification Code (RUIC) Hierarchy**

Users are advised to follow the procedures outlined in the Reserve Headquarters System (RHS) Users' Manual, October 2009 as coordinated with Commander, Navy Reserve Forces Command (CNRFC) Force Structure.

3. **Personnel Support Detachment (PSD) Pay Personnel Unit Identification Code (PPUIC)/Supported Customer Command Unit Identification Code (UIC) Hierarchy**

   a. PSD cannot see a customer UIC. If an authorized user at a PSD cannot see a customer UIC, then their required action will be:

      1) Verify in NSIPS that the UIC is reflecting as a valid UIC under that PSD.

      2) The PSD will initiate an email to NPPSC, Mr. Derek Prince describing the issue and request assistance in updating the files to reflect the PSD as the PPUIC. The following template is provided:

      Description of issue: (*example: We gained an officer to UIC XXXXX yesterday. According to NSIPS (unit administration), the UIC was valid and it reflected PSD XXXXXXX as the servicing PPSUIC (XXXXX). However, in today's reject report, the gain rejected due to error code BEY (invalid UIC). Gain did not post in L0OG and the LG line did not update in MMPA)*

      Request assistance in resolving this UIC issue. Here's the info for this UIC:

      CUSTOMER COMMAND UIC:

      COMMAND ADDRESS :

      PPSUIC/ADSN:

      COMMAND TELEPHONE NUMBER (COMM):

      MESSAGE PLAD:

      Note: AMF1 does not contain any of the above data for this UIC.

3) NPPSC will verify the data and send an email to POCs at CNPC (PERS-4013), SPAWAR ATLANTIC (NSIPS) and DFAS requesting to update UIC in question in all pay and personnel systems to reflect the proper PSD (PPSUIC/ADSN) as the servicing PSD.

4) PERS-4013, NPPSC, SPAWAR ATLANTIC and DFAS POCs will update the information.

5) If an OMPF document is urgently needed, then the normal procedures in place today for a command to obtain a copy will be adhered to. *Refer to MILPERSMAN 1070-150, Requests for Copies of the Permanent Personnel Record.*

b. Updating the PPUIC/Accounting & Disbursing Station Symbol Number (ADSN) for deploying units.

Users who are required to update the PPUIC pre and post-deployment are advised to refer to the **Navy Standard Integrated Personnel System (NSIPS) Sailor Diary Access and Navigation on Ship Server Users' Guide** available on Navy Knowledge Online (NKO).

Users are cautioned to ensure that all documents for the UIC have been released or processed in NSIPS prior to performing the UIC "shift".

6 Appendix

6.1 Default Administrator (Admin) Access Users

Table 1: Designated Billet Navy Officer Billet Classifications.

BILLET TITLE	BILLET NOBC
COMMANDING OFFICER, FLEET MARINE FORCE COMPANY	0055
COMMANDING OFFICER, NAVAL CONSTRUCTION FORCES	4305
EXECUTIVE OFFICER, NAVAL CONSTRUCTION FORCES	4310
OFFICER IN CHARGE, NAVAL CONSTRUCTION BATTALION UNIT	4340
OFFICER IN CHARGE, AVIATION UNIT OR DETACHMENT	8653
SQUADRON COMMANDING OFFICER	8670
SQUADRON EXECUTIVE OFFICER	8672
COMMANDER, OPERATING FORCES COMMAND	9005
COMMANDER, OPERATING FORCES (SELECTED)	9006
CHIEF OF STAFF	9015
CHIEF STAFF OFFICER	9016
COMMANDING OFFICER, AFLOAT	9222
EXECUTIVE OFFICER, AFLOAT	9228
COMMANDING OFFICER, AFLOAT (LIEUTENANT)	9233
COMMANDING OFFICER, AFLOAT (LIEUTENANT COMMANDER)	9234
COMMANDING OFFICER, AFLOAT (COMMANDER)	9235
COMMANDING OFFICER, AFLOAT (CAPTAIN)	9236
OFFICER IN CHARGE, AFLOAT	9273
OFFICER IN CHARGE, COMBAT CRAFT	9279
COMMANDING OFFICER, SPECIAL WARFARE TEAM	9290
EXECUTIVE OFFICER, SPECIAL WARFARE TEAM	9291
OFFICER IN CHARGE, NAVAL SHORE ACTIVITY	9420
COMMANDER/COMMANDING OFFICER, SHORE ACTIVITY	9421
COMMANDING OFFICER, NAVAL SHORE ACTIVITY (SELECTED)	9422
EXECUTIVE OFFICER, SHORE ACTIVITY	9436
COMMANDING OFFICER, MILITARY SEALIFT COMMAND OFFICE	9470
EXECUTIVE OFFICER, MILITARY SEALIFT COMMAND OFFICE	9471
MILITARY SEALIFT COMMAND COMMANDER	9950
DEPUTY/VICE COMMANDER	9992

Table 2: Designated Distribution Navy Enlisted Classifications (DNECs).

BILLET TITLE	DISTRIBUTION NEC
COMMAND MASTER CHIEF (CMDCM)	9580
CHIEF OF THE BOAT (COB)	9579
COMMAND SENIOR CHIEF	9578

6.2 PSD Personnel Pay Unit Identification Codes (PPUICs)

Access Control Lists (ACLs) for a Personnel Support Detachment (PSD) or Customer Service Desk (CSD) and associated customer commands were established by associating the PPUIC identified for the command in the Navy Activity File. The following PSD PPUICs were used.

PPUIC	ADSN	COMMAND
40065	0637	PSD AFLOAT ATLANTIC
42557	1101	WASHINGTON DC
42554	1104	BETHESDA MD
42558	1106	FT MEADE MD
42325	1109	PATUXENT RIVER MD
44175	1112	DAHLGREN VA
43100	2101	CORPUS CHRISTI TX
43105	2110	NSA NEW ORLEANS LA
43106	2201	NTC GREAT LAKES IL
43102	2202	RTC GREAT LAKES IL
43322	2208	NSA MEMPHIS TN
43084	2703	GULFPORT MS
43081	2705	PENSACOLA FL
43350	3103	WPNSTA CHARLESTON SC
43353	3104	BEAUFORT SC
43351	3107	ATLANTA GA
43352	3108	ATHENS GA
43043	3201	JACKSONVILLE FL
42975	3202	MAYPORT FL
42976	3205	KINGS BAY GA
44395	3208	TAMPA FL
43324	3209	MERIDIAN MS
43315	3302	WILLOW GROVE PA
43339	3401	NEW LONDON CT
43341	3404	SARATOGA SPRINGS NY
43343	3405	BRUNSWICK ME
43099	3409	NEWPORT RI
68548	3501	DAM NECK VA
68550	3502	OCEANA VA
68551	3503	PORTSMOUTH VA
42575	3506	LITTLE CREEK VA
42574	3508	NAVSTA NORFOLK VA
43354	3509	CAMP LEJEUNE NC
43332	3510	GUANTANAMO BAY CU
40396	3522	BAHRAIN

PPUIC	ADSN	COMMAND
43383	5102	SEOUL KOR
43384	5103	MISAWA JA
43386	5105	SASEBO JA
43387	5106	YOKOSUKA JA
43382	5108	ATSUGI JA
43385	5109	OKINAWA KADENA JA
43601	5116	IWAKUNI JA
49700	5117	SINGAPORE
43603	5122	CHINHAE KOR
43104	5301	PEARL HARBOR HI
43469	5503	DIEGO GARCIA
43462	5509	NAVSTA GU
43150	5604	BANGOR (KITSAP) WA
43138	5607	WHIDBEY ISLAND WA
43136	5608	EVERETT WA
68556	5902	NAVSTA SAN DIEGO CA
68555	5903	BALBOA CA
68554	5904	POINT LOMA CA
42827	5905	NORTH ISLAND CA
43118	5908	CAMP PENDLETON CA
43146	5911	PORT HUENEME CA
49330	5918	OKLAHOMA CITY OK
43075	5921	FALLON NV
43077	5922	LEMOORE CA
43073	5923	MONTEREY CA
3500B	5930	PSD AFLOAT WEST
43496	7111	NAPLES IT
43498	7112	ROTA SP
43497	7113	SIGONELLA IT
44013	7115	SOUDA BAY GR
43609	7302	VAIHINGEN GE

6.3 Officer Official Military Personnel File (OMPF) Field Codes

Documents filed in the officer permanent personnel record are placed in 1 of 19 categories based on type of information in document as outlined in MILPERSMAN 1070-020 and the EMPRS TR Retain/Delete List. Each category is assigned a unique field code to allow grouping, or control of access to, documents by type.

Field Code	Categories
01	Assignment Officer Code (AOC) (currently not used)
02	photograph, most recent one
03	fitness reports
04	decorations, medals, and awards
05	educational data/transcripts
06	qualifications
07	letters of appointments and promotions
08	reserve status
09	service determination, separation, and retirement
10	miscellaneous professional history
11	security investigations and clearances
12	emergency data
13	record changes
14	personal background data
15	miscellaneous personal data
16	orders
17	privileged information, adverse material, family advocacy program, medical boards, physical evaluation boards, prisoner of war (POW) data, etc.
18	enlisted record for officer with prior enlisted service
98	closed field service record, misc correspondence

6.4 Enlisted Official Military Personnel Files (OMPF) Field Codes

Documents filed in the enlisted permanent personnel record are placed in 1 of 17 categories based on the type of information in the document as outlined in MILPERSMAN 1070-080 and the EMPRS TR Retain/Delete List. Each category is assigned a unique field code to allow grouping, or control of access to, documents by type.

Field Code	Categories
30	procurement, enlistment/reenlistment data
31	classification and assignment
32	administrative remarks
33	separation and retirement
34	miscellaneous professional service history
35	enlisted performance data
36	training and education
37	decorations, medals, and awards
38	adverse information
39	emergency data/beneficiary slips
40	record changes
41	security clearances and investigations
42	security miscellaneous
43	medical data
44	out of service inquiries/response
45	miscellaneous personal data
99	closed field service record, misc correspondence

6.5 OMPF-Command View Frequently Asked Questions (FAQs)

1. What is the purpose of the OMPF-Command View application?

The purpose of the OMPF-Command View is to provide commands access to legacy Officer and Enlisted record information not available in the Electronic Service Record (ESR) and Career Information Management System (CIMS) modules within Navy Standard Integrated Personnel System (NSIPS), and other official data sources such as the Enlisted Distribution Verification Report (EDVR).

The OMPF-Administrator (Admin) Access application allows the command to manage the User roles for the OMPF-Command View application as well as audit access to OMPFs.

2. Who should have access to the OMPF-Command View application?

All military personnel record information is classified as **"For Official Use Only"** with Protected Personal Information (PPI) covered by the Privacy Act. Personnel entrusted with access to Official Military Personnel File (OMPF) information must have the appropriate active security investigation and should be familiar with the references listed in the appendix of the OMPF-Admin Access and OMPF-Command View Users' Guide.

In addition, personnel data is to be accessed and/or used **only** for official actions in the performance of personnel administrative tasks and is only to be disclosed to authorized persons conducting official military business.

3. How do I get access?

Refer to Supporting Processes outlined in the OMPF-Admin Access and OMPF-Command View Users' Guide available on the CNPC website at HTTP://WWW.NPC.NAVY.MIL/CAREERINFO/RECORDSMANAGEMENT/OMPF_CMDVIEW.HTM.

4. What documents are viewable through the OMPF-Command View application?

OPMF documents in "Non-controlled" Records within the authorized Users Access Control List based on the user role assigned.

> Officer Users – have access to documents in Officer Field Codes 01, 02, 04 through 16, 18 and 98 as well as Enlisted Field Codes 30 through 43, 45, and 99.
>
> Enlisted, Civilian and Contractor Users – have access to documents in Enlisted Field Codes 30 through 43, 45, and 99

Refer to the MILPERSMAN articles 1070-020 and 1070-080 for more field code information.

5. How do I know who has viewed my OMPF?

Admin Access and Delegated Admin Users for your command have access to an Audit tool which tracks which OMPF documents each User has viewed.

6.6 Acronyms and Abbreviations

The following acronyms and abbreviations are used in this document:

ACL	Access Control List
ADMIN UIC	Administrative Unit Identification Code
ADSN	Accounting and Disbursing Symbol Number
BA	Billets Authorized
CSD	Customer Service Desk
DNEC	Distribution Navy Enlisted Classification
EMPRS TR	Electronic Military Personnel Records System Technical Refresh
ESR	Electronic Service Record
FSR	Field Service Record
OMPF	Official Military Personnel File
NAVACTSTAT	Navy Activity Status File
NAVPERS	Navy Personnel
NOBC	Navy Officer Billet Classifications
NPC	Navy Personnel Command
NPDB	Navy Personnel Data Base
NSIPS	Navy Standard Integrated Personnel System
OMPF	Official Military Personnel File
PSD	Personnel Support Detachment
PPI	Protected Personal Information
PPUIC	Pay Personnel Unit Identification Code
RIS	Readiness Information System
RHS	Reserve Headquarters System
RUIC	Reserve Unit Identification Code
TFFMS	Total Force Manpower Management System
UIC	Unit Identification Code

6.7 References

Government Paperwork Elimination Act (GPEA, P.L. 105-277)

Section 552 of Title 5 United States Code, The Freedom of Information Act

DOD Directive 5015.2, Department of Defense Records Management Program, March 2000

DODD 4300.07, Department of Defense Freedom of Information Act (FOIA) Program, January 2008

DOD 5400.7-R, Department of Defense Freedom of Information Act (FOIA) Program, September 1998

DOD 5400.11-R, Department of Defense Privacy Program, May 2007

SECNAVINST 5211.5E, Department of the Navy (DON) Privacy Program, December 2005

OPNAVINST 1000.16K, Navy Total Force Manpower Policies Procedures, August 2007

OPNAVINST 5400.44, Navy Organization Change Manual, October 2008

OPNAVNOTE 5400 Ser DNS-33/10U107437, Standard Naval Distribution List (SNDL), March 2010

OPNAVINST 1000.23C, Pay/Personnel Administrative Support System (PASS) Management Manual (PASSMAN), June 2007

BUPERSINST 1070.27C, Document Submission Guidelines for the Electronic Military Personnel Records System (EMPRS), November 2010

NAVPERS 16000, *Total Force Manpower Management System (TFMMS) Data Dictionary*

NAVADMIN 292/06, Implementation of the Electronic Service Record

NAVADMIN 043/09, Mandatory Use of the Navy Standard Integrated Personnel System (NSIPS) Electronic Service Record (ESR)

COMNAVRESFORINST 1001.5E Ch 3, Administrative Procedures for the Drilling Reserve and Participating Members of the Individual Ready Reserve, April 2006

The Navy Officer Manpower and Personnel Classifications Volume I, April 2010

The Manual of Navy Enlisted Manpower and Personnel Classifications and Occupational Standards Volume II, April 2010

NAVPERS 15560D, Naval Military Personnel Manual (MILPERSMAN), August 2002

Specifically:

MILPERSMAN 1070, Personnel Records

- MILPERSMAN 1070-020, Officer Permanent Personnel Record
- MILPERSMAN 1070-080, Enlisted Permanent Personnel Record

COMNAVPERSCOMINST 5000.1 Article 0110-510, May 2007 (not available to all)

*Readiness Information System (RIS) Users' Manual***,** April 2001

Reserve Headquarters System (RHS) Users' Manual, October 2009