CO Decision Support: OMPF and ESR Command Views

This reference is designed for the **Commanding Officer**.

Within policy guidance established for user access to military service records, the Commanding Officer chooses which Command Stakeholders will be granted OMPF and ESR Command View access to online personnel information. This is a command decision that should not to be delegated.

The primary purpose for this user aid is to provide information supporting the decision-making process.

BACKGROUND

The Official Military Personnel File (OMPF) contains electronic images of documents generated throughout the career of every Navy officer and enlisted member, from time of entry until final separation.

- Individual Fleet users (officer and enlisted) automatically have access to their official record via the OMPF My Record view.
- Commanding Officers, Officers-in-Charge, Executive Officers and Command Master Chiefs/ Chiefs of the Boat automatically have access to OMPF records belonging to members of their command via the OMPF Command View.
- Using inherent administrator rights, the CO/OIC, XO, CMC/COB may delegate an Administrator Access User who can then establish and manage OMPF Command View accounts for stakeholders such as the Personnel Officer, Career Counselor, Legal Officer, etc.[1]

The Navy Standard Integrated Personnel System (NSIPS) / Electronic Service Record (ESR) is replacing the paper Field Service Record (FSR) previously maintained by the command or servicing Personnel Support Detachment (PSD). Information that used to be entered on documents filed in the FSR is now entered as electronic data in the NSIPS ESR.

- Individual Fleet users (officer and enlisted) may establish access to ESR data via the ESR Self-Service view.
- Commanding Officers, Officers-in-Charge, Executive Officers, Administrative Officers, Command Master Chiefs/Chiefs of the Boat, and Command PASS Coordinators (E-6/GS-6 and above) may establish access to ESR data belonging to members of their command via the ESR Administrative View. Note, Commanding Officers must endorse any SAAR submitted by a stakeholder outside the CO/XO/CMC/AO/CPC group authorized by NAVADMIN 292/06.

WHAT WILL A STAKEHOLDER WITH COMMAND VIEW ACCESS SEE?

OMPF Command View provides access to service record documents for personnel assigned to the UIC(s) for which access is granted. Access is limited to specific documents and depends on whether the stakeholder is officer or enlisted. See *OMPF - Command View Users' Guide*[2] to identify which documents can be viewed.

ESR Administrative View provides access to all service record data for all personnel assigned to the UIC(s) for which access is granted, with the exception of officer FITREP data. In other words, a command stakeholder with NSIPS/ESR Administrative View access can view personnel data for everyone assigned to the UIC(s), officer and enlisted.

Commands will use ESR Administrative View for many stakeholder tasks. At times, however, it may become necessary to obtain additional information via OMPF Command View. Information found in OMPF but not in ESR includes Eval/FITREP narrative remarks, letters of extension for Eval/FITREP, SGLI/FSGLI election forms and certificates, Montgomery GI Bill contribution forms, and Personnel Reliability Program documents.

COMMANDING OFFICER DECISION REQUIRED

The Commanding Officer must decide whether or not to provide access to command stakeholders. The following chart will help. In the left-hand column find the command stakeholders who typically

1 Commanding Officers, Officers-in-Charge, Executive Officers and Command Master Chiefs/Chiefs of the Boat have automatic OMPF Command View access to UIC-specific records based on Billet Sequence Codes containing specified Navy Officer Billet Classification (NOBCs) and Distribution Navy Enlisted Classification (DNECs) Codes. Using inherent administrator rights, one of the above may delegate an Administrator Access User who will then establish and manage command stakeholder access.
2 View, download and print from NPC (http://www.npc.navy.mil) > Career Info > Records Management > OMPF - Command View.

perform tasks that require a view of personnel information. Then review two options for granting access to ESR and two for granting access to OMPF.[3] Option A limits access to the fewest stakeholders; Option B provides access to more stakeholders. The commanding officer may decide to use either, none, or a combination of options based on the following criteria:

- Stakeholder performs tasks that require access to personnel information, including PII.
- Stakeholder has a "need to know".

Command Stakeholder	NSIPS/ESR Administrative View For more information: QuickStart for ESR Administrative View		OMPF Command View For more information: QuickStart for OMPF Command View	
	ESR Option A	ESR Option B	OMPF Option A	OMPF Option B
CO/XO/CMC/COB	✓	✓	✓	✓
Dept Head, Division Officer				
LCPO				
Admin Officer, Personnel Officer	*NSIPS Personnel Supervisor role provides capability for field level data verification and view of all ESR records.*		✓	✓
Pers/Pay Clerk, Cmd PASS Coord (Admin rating)	*NSIPS Personnel Clerk role provides capability for field level data entry and view of all ESR records.*		✓	✓
Cmd PASS Coord (non-Admin rating)	✓	✓		✓
Cmd IA Coord		✓		✓
Career Counselor	*NSIPS/CIMS CCC role provides capability for field level data entry and view of all ESR records.*		✓	✓
Training Officer				
ESO				
Legal, Master-at-Arms, NCIS Agent		✓		✓
DAPA				
Security Manager		✓		✓

The final decision regarding stakeholder access to online personnel records must be made by the Commanding Officer.

Remember, access to OMPF and ESR equals access to online personnel records. When command policy is liberal, more stakeholders have flexibility in performance of their duties, although PII becomes more vulnerable. When command policy is conservative, protection of PII is increased but the ability for some stakeholders to perform assigned tasks may become more difficult.

Regardless of option selected, commands must establish business rules that support stakeholders in the performance of their duties (see "Accountability" page 4). At a minimum, stakeholders without access to ESR and OMPF records must receive support from stakeholders who do have access. Stakeholders may request assistance from their servicing PSD (via the Command PASS Coordinator) or Personnel Office, as well.

Supporting information

- Excepts from Department of the Navy (DON) Chief Information Officer (CIO) guidance regarding

3 Remember, NSIPS/ESR contains personnel data and OMPF contains personnel documents. Stakeholder tasks may necessitate access to both systems, as well as to documents maintained in command retain files ("junk jackets").

protection of Personally Identifiable Information (PII) are provided in this user aid, pages 3-4. Designated Command Stakeholders should use the *QuickStart for OMPF Command View* and *QuickStart for ESR Administrative View*, both available online:

- NPC (http://www.npc.navy.mil) > NPC Quick Links > Career Toolbox > Command Leadership
- NKO (https://wwwa.nko.navy.mil) > Career Management > Navy Career Tools

- Also on NPC and NKO is an EXCEL document providing the following information:
  - Inventory of documents previously maintained in the FSR with cross-reference to OMPF and NSIPS/ESR data, plus indication of whether or not the information is available in electronic form.
  - Recommendation for specific documents the command should retain in paper form.
  - Recommendation for specific documents the Sailor should retain in paper form.
  - List of command stakeholders, stakeholder tasks (per Navy policy or tradition), and personnel documents/data required to support stakeholder duties and responsibilities.

COMMAND REQUIREMENT TO PROTECT PII

What information found in Navy personnel records constitutes PII?

Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity. Examples include, but are not limited to: name, Social Security number (SSN), date of birth, home address, home phone number, personal email address, family data, religion, race, national origin, fingerprints, photographs, performance ratings, security clearance level, leave balances, types of leave used, financial information, and medical information. For a complete definition of PII, go to "What is PII?" at http://www.doncio.navy.mil/contentview.aspx?id=2428

IMPORTANT: Full and partial SSNs associated with a name are especially sensitive and commonly found on many service record documents. Special care should be taken to safeguard these sensitive personal elements and all medical and financial information from persons without a need to know. In all circumstances, command stakeholder access to PII should be based on "need to know" in the performance of assigned tasks.

A special warning regarding transfer of PII via unencrypted email:

It is IMPERATIVE that command stakeholders encrypt email containing PII within the email subject line, email text and/or email attachments. Any transmission of unencrypted PII is considered a PII breach and must be reported within one hour of discovery in accordance with DON CIO MESSAGE DTG: 291652Z FEB 08, "Loss of Personally Identifiable Information (PII) Reporting Process".

The Department of the Navy (DON) Chief Information Officer (CIO) message and PII Breach Reporting Resources are available on the DON CIO website at http://www.doncio.navy.mil/ContentView.aspx?id=852

ELEMENTS OF A GOOD PRIVACY PROGRAM (EXCERPTS)

The following business rules and best practices will help command leadership protect PII belonging to members of the command. Content is derived from resources provided by DON CIO. To review original source material:

- Go to http://www.doncio.navy.mil/ContentView.aspx?ID=906
- View *Elements of a Good Privacy Program* (October 2010) and *Elements of a Good Privacy Program (Part Two)* (November 2010).

Seven elements provide the basis for a robust command privacy program:

1. Leadership

- Command leadership should establish a privacy program that considers privacy protections and controls when making business decisions involving the collection, use, sharing, retention, disclosure and destruction of personally identifiable information (PII), whether in paper or electronic form. Specifically, command leadership will implement policy governing creation, custody, use and management, and dispositioning of command retain files (also known as "junk jackets"), whether paper or electronic.
- Command should designate a Privacy Act coordinator or a privacy official who can develop and implement command policies, based upon SECNAVINST 5211.5E, DON Privacy Program.

2. Privacy Risk Management and Compliance Documentation

- Command leadership is accountable for identifying privacy risk in its business processes and IT systems and for implementing mechanisms to ensure organization documents are in compliance with laws, regulations, and policies governing the protection of privacy.
- Corrective action should be taken immediately where vulnerabilities exist. Personal accountability actions should be taken when applicable.
- Command leadership should apply a risk-based approach to the management of privacy.

3. Information Security

- Command leadership is accountable for protecting PII they collect, use, share, retain, disclose, turn-in and physically destroy, through appropriate administrative, technical and physical safeguards.
- The Privacy Act coordinator must direct action to minimize the collection and/or retention of PII to information that is necessary and relevant to the mission. This is important to mitigate the risk of information being compromised, inadvertently exposed or stolen.
- If the command does not need the data, then it should not be collected. In this instance, a “less-is-more” approach will enhance information security.
- Retention, disposition and destruction schedules that support the goals of privacy and security must be established and enforced in accordance with SECNAV M-5210.1, DON Records Management Manual.

4. Incident Response

- Command leadership is accountable for having a robust plan for managing incidents involving the potential or actual leakage of PII that includes notification to appropriate DON leadership and affected personnel (including Navy dependents) where appropriate.

5. Notice and Redress for Individuals

- Command leadership is accountable for providing transparency through clear notice to personnel about the organization’s information handling practices and mechanisms for individual participation to ensure appropriate access, correction and redress regarding the use of PII.

6. Privacy Training and Awareness

- Command is accountable for ensuring all personnel under their control successfully complete annual PII training, and are familiar with DON Privacy Program required procedures, practices and documents.
  - A best practice is that all personnel must successfully complete privacy training before being permitted access to DON information and information systems.
  - Annual training requirement can be met via Navy eLearning course.
- Additional or advanced training should be provided to stakeholders commensurate with increased responsibilities or change in duties.
  - Personnel who cause or commit a PII breach are required by DON to take PII refresher training with documented completion for every reportable breach.
  - Advanced/refresher training can be achieved via Navy eLearning course.
- Both annual and PII refresher training should include acceptable rules of behavior and consequences when the rules are not followed.

7. Accountability

- Command is accountable for compliance with all applicable privacy protection requirements, including all legal authorities and established policies and procedures that protect privacy and govern the collection, use, dissemination and maintenance of PII.
- All command stakeholders will safeguard PII.
  - All command stakeholders with access to PII will comply with 5 U.S.C. § 552a, The Privacy Act of 1974; DoD 5400.11-R, DoD Privacy Program; SECNAVINST 5211.5E, DON Privacy Program; and SECNAV M-5210.1, DON Records Management Manual.
- A best practice is to designate stakeholders in letter form and/or signed Page 13 entry:
  - Identify duties and responsibilities regarding access to and use of personnel information based on need to know.
  - Clearly articulate requirement to protect Sailor PII.