**Recall Rosters** (Organizational and Office Rosters)

Records, Privacy, and Declassification Division

Information Paper

Recall rosters serve a useful and valid purpose for contacting individuals in order to recall personnel, notify them of building/base/office closings, and other important occurrences. Safeguards must be in place to ensure that the personally identifiable information (PII) they contain is properly maintained and protected to prevent inadvertent disclosure. PII breaches can occur due to the mishandling of recall rosters. Examples of this include rosters being posted in publicly accessible areas; rosters being transmitted as email attachments without proper encryption and marking; rosters stored on a shared drive without the appropriate access controls in place; and failure to protect hard copy rosters outside the workplace.

These privacy tips provide specific safeguards all Department of Defense (DoD) personnel should use when creating and sharing recall rosters.

* Ask: Does the recipient(s) have a need to know? Is the information appropriately marked as "FOUO - Privacy Sensitive"? Is the transmission secure/encrypted? Should the information be displayed in this location? Are only essential PII elements listed?
* Establish procedures for proper maintenance, storage and dissemination.
* Provide training to ensure DoD personnel follow established procedures.
* Limit PII elements to only the minimum required, e.g., names, addresses telephone numbers (home, work, cell) and/or email address. The SSN, date of birth, or DoD ID Number should never be included.
* Post all rosters to an intranet site only when proper access controls are in place.
* Provide a Privacy Act Statement (PAS) any time PII is solicited from an individual, whether in writing or electronically. Contact your Privacy Officer for more information. (See below PAS example).
* Ensure that compliance spot checks include recall rosters.
* Ensure that the sole purpose of a recall roster is to recall personnel, notify them of building/base/office closings, and other important occurrences.

**PRIVACY ACT STATEMENT (EXAMPLE)**

# **AUTHORITY:** Cite and write out titles the authorities identified in the applicable SORN’s “Authorities” category.

**PRINCIPAL PURPOSE:** State the same purpose identified in the SORN’s “Purpose” category.

# **ROUTINE USE:** List the same routine uses that are identified in the SORN; however, if the routine uses are too many to list in the privacy act statement, the statement “see the application system of records notice for additional routine uses” can be used. Give the system ID, name and link to the system of records notice here.

**DISCLOSURE:** Cite whether or not the disclosure of information is "Voluntary" or "Mandatory". If furnishing information is a condition for granting a benefit or privilege voluntarily sought by the individual, it is “Voluntary” for the individual to give the information. It is only appropriate to cite "Mandatory" when a Federal Law or Executive Order of the President specifically imposes a requirement to furnish the information and provides a penalty for failure to do so.