

EMAIL SUBMIT	<h2 style="margin:0;">SSN REDUCTION REVIEW</h2> Submission for <i>(Check one)</i> : <input checked="" type="checkbox"/> FORM <input type="checkbox"/> IT SYSTEM	DATE COMPLETED: <u>22 Feb 2017</u>
Form Number: <u>SECNAV 5512/1</u>		Requiring Document: <u>see Authorities in section 2 below</u>
Form Revision Date: <u>03/31/2017</u>		

SECTION 1

**TO BE COMPLETED BY FORM ORIGINATOR/SPONSOR. Forms that collect and retrieve by SSN/PII must be covered by a System of Record Notice (SORN), be call for within a requiring document, and have Privacy Act Officer approval for Privacy Act Statements. Return completed packages that contain the SSN Reduction Review Form, Justification, and if need the DD 67 and the SSN Elimination Plan to the cognizant forms manager. If SECNAV/OPNAV/NAVSO send to DON Forms Manager OPNAV. DONFORMS.DNS51@navy.mil, If NAVMC forms send to the USMC Forms Manager, SMB.HQMC.ARDE@USMC.MIL**

- |  |   |
|--|---|
| 1. Is the form covered by a System of Record Notice (SORN)?                                    | <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO |
| a. If yes, what is the SORN number? <u>NM05512-2 and DMDC 16</u>                               |   |
| b. If no, contact the Privacy Act Officer for instructions.                                    |   |
| 2. Does the form contain a Privacy Act Statement (PAS)?  | <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO |
| a. If yes, has the PAS been approved by a Privacy Act Officer?                                 | <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO |
| b. If no, contact the Privacy Act Officer for instructions.                                    |   |
| 3. Is the SSN Field needed?  | <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO |
| a. If no, complete DD67 to request revision of the form.                                       |   |
| 4. Is this form electronic?  | <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO |
| a. If yes, is the SSN field masked or truncated?   | <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO |
| b. If no, could it be?   | <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO |
| 5. Is this form part of an IT system?  | <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO |
| a. If yes, what is the IT System name and DITPR DON ID? <u>NACS - 23212; and BAACS - 22557</u> |   |
| b. If yes, does the IT System mask or truncate the display of the SSN on the form?             | <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO |
| c. If no, Could it be?   | <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO |
| 6. Is Justification Memorandum for the Record attached?  | <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO |
| 7. Could an alternative to the SSN be used?  | <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO |

CONTACT INFORMATION - IT System Owner or Form Originator/Sponsor

Name, Code, Mailing Address Charles Pierce, PP&O (PS), Pentagon Room 4A324, Washington, DC 20350	Office Telephone Number: (703)695-7202
	E-mail Address charles.a.pierce1@usmc.mil

SECTION 2 TO BE COMPLETED BY PRIVACY ACT OFFICER

**To verify information given in Section 1 is accurate, is in compliance with Privacy Act Regulations, and meets requirements of the SSN Reduction Plan.**

- |  |   |
|--|---|
| 1. Is Privacy Act Statement (PAS) correct?   | <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO |
| 2. If there is not a PAS, is one needed?   | <input type="checkbox"/> YES <input type="checkbox"/> NO            |
| 3. If a PAS needed, what is the correct PAS? (Originator/owner of form/IT system will work with the Privacy Act Officer to draft a PAS if needed) (Field will expand to fit typed data)) |   |

**PRIVACY ACT STATEMENT:**

**AUTHORITY:** 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB); DoD 5200.08-R, Physical Security Program; DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense (Exception to policy memos); Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control; DTM 14-005, DoD Identity Management Capability Enterprise Services Application (IMESA) Access to FBI National Crime Information Center (NCIC) Files; E.O. 9397 (SSN), as amended; OPNAVINST 5530.14E, Navy Physical Security and Law Enforcement Program; Marine Corps Order 5530.14 Marine Corps Physical Security Program Manual; SORN NM05512-2 and DMDC 16 <http://dpcl.d.defense.gov/Privacy/SORNsIndex>

**PURPOSE(S):** To control physical access to Department of Defense (DoD), Department of the Navy (DON) or Marine Corps installations/units, controlled information, installations, facilities, or areas over which DoD, DON, or Marine Corps has security responsibilities by identifying or verifying an individual through the use of biometric databases and associated data processing/information services for designated populations for purposes of protecting U.S./coalition/allied government/national security areas of responsibility and information; to issue badges, replace lost badges, and retrieve passes upon separation; to maintain visitor statistics; collect information to adjudicate access to facility; and track the entry/exit times of personnel.

**ROUTINE USE(S):** To designated contractors, federal agencies, and foreign governments for the purpose of granting Navy officials

access to their facility.

**DISCLOSURE:** Providing registration information is voluntary. Failure to provide requested information may result in denial of access to benefits, privileges, and DoD installations, facilities and buildings.

4. Is the System of Records Notice (SORN) number cited in Section 1 correct?  YES  NO

5. Does a SORN need to be initiated?  YES  NO  
*(Determination of need for SORN will be worked between the originator/owner of form/IT system and Command Privacy Act Office)*

6. Is use of SSN Justification Form complete and approved?  YES  NO

<input checked="" type="checkbox"/> APPROVED	<u>Deborah Contaoi</u>	<u>17 Mar 2017</u>
<input type="checkbox"/> DISAPPROVED	Privacy Act Officer Printed Name	Privacy Act Officer Signature
		Date

SECTION 3 - COMMAND FORMS MANAGER

<input checked="" type="checkbox"/> APPROVED	<u>Ernest W Williams</u>	<u>17 Mar 2017</u>
<input type="checkbox"/> DISAPPROVED	Forms Manager Printed Name	Forms Manager Approval Signature
		Date:

**NOTES:**

- (1) If Disapproved, sponsor/originator will need to provide a plan to include milestones and timeline of the elimination of the SSN usage.
- (2) SSN Reduction Packages for forms will be kept by the cognizant form manager in the forms's history/case file.
- (3) SSN Reduction Packages for IT Systems will be kept by the cognizant CIO office.

22 Feb 2017

Date

## MEMORANDUM FOR THE RECORD

Subj: JUSTIFICATON FOR THE USE OF THE SOCIAL SECURITY NUMBER (SSN)

SECNAV 5512/1 DON LOCAL POPULATION ID CARD/BASE ACCESS PASS RE*(Form number and name or IT system name and DITPR DON ID number)*

The DEPARTMENT OF THE NAVY LOCAL POPULATION ID CARD/BASE ACCESS PASS REGISTRATION, SECNAV 5512/1, is utilized by U.S. Navy and Marine Corps installations as an authorized OMB collection instrument under OMB 0703-0061 and is required in support of Physical Access Control and Physical Security missions. SECNAV 5512/1 is used to collect identity information from those individual respondents requesting physical access who are not otherwise credentialed under DoD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," December 5, 1997. The respondent voluntarily provides their identity information on a SECNAV 5512/1 form, and submits it in person to the Navy/USMC registrar who is required to enter specific identity information into criminal justice information systems, as required, to perform a background check to determine the fitness of the respondent who is requesting access to DOD or DON installations. If a background check results in a finding that the respondent is fit to access the base, the Navy/USMC registrar is required to enter specific identity information including the SSN into the Navy or USMC Physical Access Control System as required to issue a Local Population ID Card or Base Access Pass to the respondent. The SSN is not printed or electronically encoded on the Local Population ID Card or Base Access Pass.

Operational Necessity: To control physical access to DoD, Department of the Navy (DON) or U.S. Marine Corps installations/units controlled information, installations, facilities, or areas over which the DoD, DON or USMC has security responsibilities by identifying or verifying an individual through the use of biometric databases and associated data processing/ information services for designated populations for purposes of protecting U.S./ coalition/allied government/ national security areas of responsibility and information; to register DOD identification cards and local population identification cards, replace lost ID cards and retrieve passes upon separation; to maintain visitor statistics; collect fitness determination information to adjudicate access to facility; and track the entry/exit times of personnel.

Laws or Regulations: 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB); DoD 5200.08-R, Physical Security Program; DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense (Exception to policy memos); Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control; DTM 14-005, DoD Identity Management Capability Enterprise Services Application (IMESA) Access to FBI National Crime Information Center (NCIC) Files; E.O. 9397 (SSN), as amended; OPNAVINST 5530.14E, Navy Physical Security and Law Enforcement Program; Marine Corps Order 5530.14A Marine Corps Physical Security Program Manual; SORN NM05512-2 and DMDC 16 <http://dpcl.d.defense.gov/Privacy/SORNsIndex>

DoD Directive 1000.25, "DoD Personnel Identity Protection (PIP) Program," July 2004, establishes policy for the implementation and operation of the PIP Program, to include use of DoD identity credentials and operation of DoD Physical Access Control Systems that are used by DOD joint Services.

OUSD(I) Directive Type Memorandum (DTM) 09-012 mandated that DOD Physical Access Control Systems must support a DoD-wide and federally interoperable access control capability that can authenticate USG physical access credentials and support access enrollment, authorization processes, and securely share information. The SECNAV 5512/1 has been developed to support DON compliance with the DTM 09-012 and provides DON physical security authorities with a common collection instrument and approach to support those individual respondents needing physical access who are not otherwise credentialed under DoD Instruction 1000.13. The SSN is one of the primary documents that is required to be recorded on the SECNAV 5512/1 and physically presented in order to establish Identity and Employment Authorization as is specified in the

instructions on page 3 of the SECNAV 5512/1. The SSN is one of the required data elements that is submitted to the National Crime Information Center that are used to determine fitness and confirm eligibility of individuals who are requesting access to DOD or DON installations. The SSN is also one of the primary required data dictionary elements in the DON installation's Physical Access Control System used to produce and issue a DON Local Population Identity Card/Base Access Pass and used to electronically authenticate the ID card/pass when the card is presented at DON installation access control points.

Conclusion: The SSN serves as primary identity information that is required to 1) establish identity; 2) determine fitness for access; and 3) register in the DON installation's Physical Access Control System in order to produce and issue a DON Local Population Identity Card/Base Access Pass. If the SSN is eliminated:

- DON will lack a common DON collection instrument;
- DON will not be fully compliant with DTM-09-012;
- DON will not have a common solution for respondents needing physical access who are not otherwise credentialed under DoD Instruction 1000.13;
- Process and paperwork duplication and disparity will occur, thereby increasing the likelihood of SSN mismanagement.
- The estimated costs associated with eliminating the SSN are undetermined at this time, however the costs would be a significant impact because of the extent of the changes that would be required to be made to the DOD authoritative data sources and DON Physical Access Control Systems that are deployed across the DON enterprise.

---

Signature (*Flag, SES, or by direction*)

Asst. Dpty Commandant, PP&O(Security)

---

Title and Code

Security Division, PP&O, HQMC

---

Command

*Note: Justification must include operational necessity, cost, etc. explanation and impact if SSN were to be eliminated)*