



Department of Defense INSTRUCTION

NUMBER 1000.30

August 1, 2012

USD(P&R)

SUBJECT: Reduction of Social Security Number (SSN) Use Within DoD

References: See Enclosure 1

1. PURPOSE. This Instruction:

- a. Establishes policy and assigns responsibilities for SSN use reduction in the Department of Defense in accordance with the authority in DoD Directive 5124.02 (Reference (a)).
- b. Establishes a DoD SSN Use Reduction Plan.
- c. Incorporates and cancels Directive-Type Memorandum 07-015 (Reference (b)).

2. APPLICABILITY. This Instruction:

- a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (IG, DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereinafter referred to collectively as the "DoD Components").
- b. Covers all uses of SSNs within the Department of Defense, in accordance with section 552a of title 5, United States Code (U.S.C.), as amended (also known and hereinafter referred to as "The Privacy Act" (Reference (c))).

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

- a. All DoD personnel shall reduce or eliminate the use of SSNs wherever possible.

b. Use of the SSN includes the SSN in any form, including, but not limited to, truncated, masked, partially masked, encrypted, or disguised SSNs.

c. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria in Enclosure 2.

d. SSNs shall be used in approved forms and systems when they meet one or more of the acceptable use criteria in Enclosure 2.

e. Specific reviews of forms and systems shall be conducted to reduce SSN use. See Enclosures 3 and 4 for review procedures.

5. RESPONSIBILITIES. See Enclosure 5.

6. INFORMATION COLLECTIONS REQUIREMENTS

a. The Federal Information Security Management Act (FISMA) reports referenced in sections 1.b.(2)(a) and 2.b.(3)(e) of Enclosure 3 have been assigned Report Control Symbol (RCS) DD-CIO(A,Q)2296 in accordance with DoD 8910.1-M (Reference (d)).

b. The Defense Privacy Program reporting requirements in sections 1.a.(2)(b) and 1.b.(1)(a) of Enclosure 3 have been assigned RCS DD-DA&M(AR)1379 in accordance with Reference (d).

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

8. EFFECTIVE DATE. This Instruction:

a. Is effective August 1, 2012.

b. Must be reissued, cancelled, or certified current within 5 years of its publication in accordance with DoD Instruction 5025.01 (Reference (e)). If not, it will expire effective August 1, 2022 and be removed from the DoD Issuances Website.



Erin C. Conaton
Under Secretary of Defense for
Personnel and Readiness

Enclosures

1. References
2. DoD Guidance on the Use of the SSN
3. DoD SSN Use Reduction in Forms and Systems
4. Approval for Use of the SSN
5. Responsibilities

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....6

ENCLOSURE 2: DoD GUIDANCE ON THE USE OF THE SSN7

 OVERVIEW7

 ACCEPTABLE USES7

 DOCUMENTING AUTHORIZED USES9

 ALTERNATIVES.....10

 DoD Identification Number10

 System-Specific Identifiers11

 Net-Centric Environment.....12

 Elimination of Identifier12

 Biometrics12

 Situational Elimination and Protection12

 TRAINING12

ENCLOSURE 3: DoD SSN USE REDUCTION IN FORMS AND SYSTEMS.....13

 DoD FORMS13

 Use of SSN in DoD Forms.....13

 Reporting Results.....14

 Schedule.....15

 DoD SYSTEMS15

 DITPR15

 DPCLO System Review Report Process16

 IG, DoD REVIEW16

ENCLOSURE 4: APPROVAL FOR USE OF THE SSN18

 ACCEPTABLE USES18

 DOCUMENTATION18

 DITPR18

 Forms18

 DoD COMPONENT CONCURRENCE19

 PLAN TO ELIMINATE USE OF THE SSN21

ENCLOSURE 5: RESPONSIBILITIES.....23

 USD(P&R).....23

 DIRECTOR OF ADMINISTRATION AND MANAGEMENT (DA&M)23

 IG, DoD.....23

 HEADS OF THE DoD COMPONENTS24

 COMMANDERS OF THE COMBATANT COMMANDS24

GLOSSARY25

 PART I: ABBREVIATIONS AND ACRONYMS25

 PART II: DEFINITIONS.....26

FIGURES

 1. Sample SSN Justification Memorandum20

 2. Sample SSN Elimination Plan22

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5124.02, “Under Secretary of Defense for Personnel and Readiness (USD(P&R)),” June 23, 2008
- (b) Directive-Type Memorandum 07-015, “DoD Social Security Number (SSN) Reduction Plan,” March 28, 2008 (hereby cancelled)
- (c) Section 552a of title 5, United States Code, as amended (also known as “The Privacy Act”)
- (d) DoD 8910.1-M, “Department of Defense Procedures for Management of Information Requirements,” June 30, 1998
- (e) DoD Instruction 5025.01, “DoD Directives Program,” October 28, 2007, as amended
- (f) President’s Task Force on Identity Theft Strategic Plan, April 2007¹
- (g) Office of Management and Budget Memorandum M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” May 22, 2007
- (h) Executive Order 9397, “Numbering System for Federal Accounts Relating to Individual Persons,” November 22, 1943, as amended
- (i) Executive Order 13478, “Amendments To Executive Order 9397 Relating To Federal Agency Use of Social Security Numbers” November 18, 2008
- (j) DoD Directive 5400.11, “DoD Privacy Program,” May 8, 2007
- (k) DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007
- (l) Sections 3501-3520² and 3541-3549, of title 44, United States Code
- (m) DoD Chief Information Officer, “DoD IT Portfolio Repository (DITPR) and DoD SIPRNET IT Registry Guidance 2007-2008,” September 6, 2007³
- (n) DoD Instruction 7750.07, “DoD Forms Management Program,” April 20, 2007

¹ Copies of document are available at: www.idtheft.gov/reports/strategicplan.pdf

² Sections 3501-3520 are also known as “The Paperwork Reduction Act”

³ Copies of document are available at: <https://ditpr.dod.mil>

ENCLOSURE 2

DoD GUIDANCE ON THE USE OF THE SSN

1. OVERVIEW

a. The SSN has been used as a means to identify and authenticate individuals. Expanded use of the SSN has increased efficiency, enabling DoD information systems and processes to interoperate and transfer information with a greatly reduced chance of errors. However, the threat of identity theft has rendered this widespread use unacceptable, resulting in the requirement that all Federal agencies evaluate how the SSN is used and eliminate its unnecessary use in accordance with President's Task Force on Identity Theft Strategic Plan (Reference (f)) and Office of Management and Budget (OMB) Memorandum M-07-16 (Reference (g)).

b. This Enclosure identifies the acceptable uses of the SSN, describes how authorized uses shall be documented, presents alternatives to using the SSN, and explains the role that Privacy Act training plays in protecting privacy information within the Department of Defense. Any uses of the SSN not provided for in this Instruction are considered to be unnecessary and shall be eliminated. Use of the SSN includes the SSN in any form, including, but not limited to, truncated (last four digits), masked, partially masked, encrypted, or disguised SSNs.

2. ACCEPTABLE USES

a. The acceptable uses of the SSN are those that are provided for by law, require interoperability with organizations beyond the Department of Defense, or are required by operational necessities. Such operational necessities may be the result of the inability to alter systems, processes, or forms due to cost or unacceptable levels of risk. Those systems, processes, or forms that claim "operational necessity" shall be closely scrutinized. Ease of use or unwillingness to change are not acceptable justifications for this case.

b. The requirement for the use of the SSN provided by Executive Order 9397 (Reference (h)) has been eliminated. No new uses of the SSN are permitted in accordance with Reference (h) as amended by Executive Order 13478 (Reference (i)). Reference (h) may be used to justify the use of the SSN as an interim measure while its use is being eliminated, but shall not by itself be used to justify continued use of the SSN.

c. This paragraph describes general categories of use that may continue to be acceptable for the SSN. General coverage of an application by one of the use cases discussed in subparagraphs 2.c.(1) through 2.c.(13) of this enclosure must also be compared with the particular way in which the SSN is used. The fact that a use case may loosely meet one or more of the justifications does not necessarily mean that a specific justification is acceptable. The specific legislative or regulatory language must be examined to determine if it is applicable. Justification for the use of the SSN to be contained in an application does not constitute authority to use the SSN in every transaction or interaction. Any transaction that includes the display, transfer, or presentation of

the SSN should be closely scrutinized to determine if some alternate form of identification or authentication may suffice.

(1) Geneva Conventions Serial Number. As of the late 1960s, the SSN has served as the Geneva Conventions serial number for the Military Services. Many of the systems, processes, and forms used by the Department of Defense categorize individuals by their SSNs. The Military Departments should begin to transition away from the SSN as the Geneva Conventions identifier as further addressed in subparagraph 4.a.(1) of this enclosure.

(2) Law Enforcement, National Security, and Credentialing. Almost every law enforcement application available to Federal, State, and local law enforcement and other criminal justice agencies reports and tracks individuals, and makes application information available to other agencies, through the use of the SSN. This includes, but is not limited to, checks of the National Crime Information Center; State criminal histories; and Federal Bureau of Investigation records checks.

(3) Security Clearance Investigation or Verification. The initiation, conduct, adjudication, verification, quality assurance, and billing fund control of background investigations and security clearances requires the use of the SSN. The SSN is the single identifier that links all of the aspects of these investigations together. This use case is also linked to other Federal agencies that continue to use the SSN as a primary identifier.

(4) Interactions With Financial Institutions. Financial institutions may require that individuals provide the SSN as part of the process to open accounts. It may therefore be required to provide the SSN for systems, processes, or forms that interface with or act on behalf of individuals or organizations in transactions with financial institutions.

(5) Confirmation of Employment Eligibility. Federal statute requires that all persons employed within the United States provide an SSN or comparable identifier to prove that they are eligible to work for or with the U.S. Government. Any system that deals with employment eligibility may contain the SSN.

(6) Administration of Federal Workers' Compensation. The Federal Workers' Compensation Program continues to track individuals through the use of the SSN. As such, systems, processes, or forms that interact with or provide information for the administration of this system or associated systems may be required to retain the SSN.

(7) Federal Taxpayer Identification Number. The application of Federal and State income tax programs rely on the use of the SSN. As such, systems that have any function that pertains to the collection, payment, or record keeping of this use case may contain the SSN. Additionally, individuals who operate corporate entities under their own name may use their SSN as the tax number for that business function.

(8) Computer Matching. Systems, processes, or forms that interact with other Government agencies may require the continued use of the SSN as a primary identifier until such time as the applications to which they are linked move to some other identifier as a primary

means for transferring, matching, or checking information. These applications shall be rigorously scrutinized to determine the availability of some other means for conducting these transactions.

(9) Foreign Travel. DoD personnel are often required to travel beyond the borders of the United States and many members often require official clearance prior to travel. Currently, the SSN is used as the identifier for these purposes.

(10) Noncombatant Evacuation Operations (NEOs). The Department of State requires that all persons repatriated to the United States as part of a NEO present their SSN as part of this process. Any systems, forms, or processes supporting NEOs may be required to process individuals using the SSN as the primary identifier.

(11) Legacy System Interface. Many systems, processes, or forms that do not meet the criteria in subparagraphs 2.c.(1) through 2.c.(10) of this enclosure for the continued use of the SSN may not be able to transition to another identifier in a timely manner due to an interface with a legacy system still using the SSN, or due to the excessive cost associated with the change. In these cases, the continued use of the SSN may be acceptable for a specified period of time, provided that formalized, written plans are in place for the migration away from the SSN in the future. Plans to alter these use cases must take into account interactions with other applications as well as all methods for entry, processing, or transfer of information from said application. It is critical that transfer away from the SSN does not cause unacceptably long interruptions to continued operations.

(12) Operational Necessity. It is not the intention of this Instruction to preclude operational capabilities. In austere or tactical environments where continuity of operations requires the use of SSN, to include the use of hard copy lists and spreadsheets, approval can be granted that supersedes normal requirements. An example of this may include a system in a tactical environment where hard copies are used in the event of a loss of power to the system. To ensure that this is only used in cases of absolute necessity, justification of this use case must be approved by the Combatant Commander. The higher risk and increased liability to Service members and the Department of Defense should be strongly considered prior to granting approval to use this category of justification.

(13) Other Cases. The previous categories may not include all uses of the SSN authorized by law. Should an application owner be able to show sufficient grounds that a use case not specified in subparagraphs 2.c.(1) through 2.c.(12) of this enclosure is required by law, that use case may continue to use the SSN. Any application that seeks to use this clause as justification must provide specific documentation in order to continue use in accordance with this provision.

3. DOCUMENTING AUTHORIZED USES

a. Any system, process, or form that collects, transfers, or retains personally identifiable information (PII) must properly document the authority for that use. This includes, but is not

limited to, justification for the collection, retention, or use of the SSN. It is unacceptable to collect, retain, or transfer PII without such justification. The authorization for use of PII is governed through DoD Directive 5400.11 (Reference (j)). In addition to the documentation required for the use of PII, the use of the SSN as part of any collection, transfer, or retention must be specifically documented and justified. This documentation shall include justification in accordance with paragraph 2.c of this enclosure as well as any specific legislative requirements for use of the SSN. The method by which this is documented shall be consistent with existing program requirements. Forms, processes, or systems, to include any locally created applications, must be properly documented. Additionally, if the SSN (or other personal identifier) is used to retrieve information, a Privacy Act system of records notice (SORN) must exist or be established prior to its use in accordance with Reference (j) and DoD 5400.11-R (Reference (k)). The Defense Privacy and Civil Liberties Office (DPCLCLO) will work with the DoD Component to develop the notice and forward to OMB for approval to publish in the Federal Register. Individuals who choose to use PII without proper documentation may be in violation of The Privacy Act and may be held accountable to the stated consequences.

b. Forms used to collect PII shall be coordinated in accordance with each DoD Component's forms management process. The DD Form 67, "Form Processing Action Request," submitted by the DoD Component to create or revise a form, shall provide the name, initials, office symbol, and telephone number of the coordinating DoD Component officer and the SORN number entered. Copies of the justification to collect PII and a SORN notice shall be included with the DD Form 67.

c. Documentation of the justification for use of the SSN shall be retained by the DoD Component.

d. SSN justification documentation shall be submitted to the DPCLCLO when a new, altered, or amended SORN is submitted for processing and completion.

e. DoD Components shall make the SSN justification documentation available upon request to all Privacy, Chief Information Officer, and Forms Management officials throughout DoD. This documentation should also be made available to the DoD Clearance Officer for information collection approvals.

4. ALTERNATIVES. One of the primary reasons that many systems, processes, and forms shifted to use of the SSN is that it provided greater efficiency and required individuals to remember a single identifier. To counteract the vulnerability that this expanded use of the SSN created, alternatives to the SSN shall be used whenever possible. The list in this section is not meant to be definitive. For assistance in situations that are not specified, contact the Defense Manpower Data Center at acossttigerteam@osd.pentagon.mil. Alternatives include:

a. DoD Identification Number

(1) The DoD Identification Number will replace the SSN as the Geneva Conventions Serial Number for the United States as all DoD identification cards are updated through their

natural lifecycle replacement. The DoD Identification Number is the common name for the Electronic Data Interchange Personal Identifier (EDI-PI).

(a) The EDI-PI is a unique personal identifier created within the Defense Enrollment Eligibility Reporting System (DEERS) for each person who has a direct relationship with DoD.

(b) The EDI-PI has previously been used as a system identifier and is present in many DoD enterprise systems.

(2) To support widespread use of the DoD Identification Number, it will be printed on all DoD identification cards. It is intended to support replacement of the SSN in most DoD processes and business needs. It shall not be used to replace the SSN in any case where the SSN is required by law.

(3) The DoD Identification Number shall only be used for DoD business purposes. This may include transactions that include entities outside DoD, so long as individuals are acting on behalf of or in support of the Department of Defense.

(a) For use in authentication transactions, an individual's name and DoD Identification Number shall be treated as a single factor. When using an individual's name and the DoD Identification Number for authentication, a second authentication factor must also be provided beyond the individual's name and DoD Identification Number.

1. The DoD Identification Number shall not be, either by itself or in conjunction with the individual's name, be considered sufficient for any level of authentication.

2. Presence or knowledge of an individual's DoD Identification Number alone shall be considered as no more significant than presence or knowledge of that individual's name. It does not constitute any level of authority to act on that individual's behalf.

(b) The DoD Identification Number may not be shared with other Federal agencies unless a Memorandum of Understanding (MOU) is agreed upon by both the DoD and the recipient agency. MOUs for sharing the DoD Identification Number will be managed and administered by the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) and must include, at minimum, these stipulations:

1. The recipient agency must agree not to share the DoD Identification Number with any other agency or outside organization without the permission of the DoD.

2. The recipient agency must agree that the DoD Identification Number will not be used for single factor authentication, but will instead be used as only a single factor in a multi-factor authentication.

b. System-Specific Identifiers. In use cases that are linked to a limited number of other applications, the best course of action may be to create a unique identifier for each of those uses. In particular, for situations in which members of the public are required to gain access to DoD

information systems, particularly on a temporary basis, this would mitigate many privacy concerns.

c. Net-Centric Environment. A growing number of systems and processes are relying on authentication of individuals with a minimum of collection and storage of PII. These systems and processes rely on an authoritative data source as the storage of this PII, and access to that information is granted on an “as needed” basis.

d. Elimination of Identifier. Many instances where the SSN is collected or used may be able to be eliminated. The technology associated with newer applications is such that it is possible to specifically identify individuals through other pieces of information, negating the need for a unique identifier. This is particularly true of closed or stand alone applications that do not interoperate with other applications.

e. Biometrics. Biometrics is an enabling tool that can be used as part of a multi-factor authentication process. As an authentication factor, biometrics leverages “something one is” (e.g., fingerprint) as opposed to “something one has” (e.g., a common access card with Public Key Infrastructure certificates) or “something one knows” (e.g., a personal identification number), and it cannot be shared or easily compromised. While biometrics first requires an initial enrollment and thus cannot perform the role of initial identification, it can be used for continuing authentication in circumstances other than network access. (See <http://www.biometrics.dod.mil/> for more information.)

f. Situational Elimination and Protection. Authority to collect, maintain, or use the SSN does not constitute blanket approval to use the SSN throughout any business process. Every associated report, display, printout, and transaction shall be reviewed to determine the appropriate authority and requirements for the use of the SSN and to determine all other required Privacy Act considerations and documentation. If upon review, it is determined that no authority or legal requirement for the use of the SSN exists, its collection and use should cease until such authority can be obtained. Where appropriate authorities and requirements exist, consideration of whether the SSN can be further protected by masking or truncating must be made.

5. TRAINING. It is vital to the Department of Defense that the collection, retention, storage, use, and disposal of PII be handled appropriately, and only by individuals who are qualified to do so and have a need to know. To ensure that all personnel, including contractors, are so trained, References (j) and (k) require that, prior to operating systems that contain or use PII, individuals be trained on appropriate handling. In addition to this use-specific training, Reference (k) requires DoD Components and subordinate organizations to have training programs that promote strong precautions and heightened awareness for the handling of PII. Properly completing and documenting this training is essential to reducing the chance of loss or breach of PII and the consequences thereof.

ENCLOSURE 3

DoD SSN USE REDUCTION IN FORMS AND SYSTEMS

1. DoD FORMS

a. Use of SSN in DoD Forms

(1) New Forms

(a) Action Officer Requirements

1. Provide justification for using SSNs. (See Enclosure 2 for acceptable uses.)
2. If justified, indicate if the SSN can be truncated or masked.
3. Identify the form's association to the SORN(s), privacy impact assessment(s) (PIA), and the DoD Information Technology Portfolio Repository (DITPR) identification number, as applicable.

(b) Approval of SSN Justifications. All SSN justifications must be signed by the appropriate authority (see section 3 of Enclosure 4 and section 4 of Enclosure 5) if continuing to collect the SSN.

(c) Requirement for Reviewing SSN Justifications

1. For DD and SD forms, the justifications shall be reviewed by the DoD Forms Management Officer, who shall consult with the DPCLO, to verify whether the justification is valid.
2. For DoD Component forms, the justifications shall be reviewed by the DoD Component to verify whether the justification is valid.
3. For command and installation forms, the justifications shall be reviewed by the DoD Component to verify whether the justification is valid.

(2) Existing Forms

(a) Review of SSN Use and Justification

1. The DoD Forms Management Officer shall conduct a review of all DD and SD forms to ensure compliance with the guidance in Enclosure 2.
2. The DoD Components shall conduct reviews of all Component forms to ensure compliance with the guidance in Enclosure 2.

3. For command and installation forms, the appropriate forms management officers shall conduct reviews to ensure compliance with the guidance in Enclosure 2.

4. Where justification for use of SSNs does not currently exist, it shall be submitted in accordance with subparagraph 1.a.(1)(a) of this enclosure.

5. Where a justification for SSN use is not accepted, the action officer will prepare a plan, to include milestones and a timeline, for the elimination of SSN usage; this process is further detailed in section 4 of Enclosure 4. The final date for SSN elimination will be provided to the DoD Forms Management Officer, through the DoD Component if applicable.

6. The review and justification of SSN use in DD forms and SD forms shall be ongoing until all forms are compliant.

(b) Periodic Review of SSN Use and Justification. The reporting of the SSN review and approval process shall be added to the biennial Privacy Act SORN review administered by the DPCLC. The frequency and manner of the reporting of these reviews shall be established in accordance with the report requirement authority in Reference (k).

b. Reporting Results

(1) New Forms

(a) For DD and SD forms, the DoD Forms Management Officer shall maintain a database to produce an annual report as of July 1. This report shall be included in the annual report required by section 3544(c) of title 44, U.S.C. (Reference (l)) and compiled by the DPCLC. The annual report shall contain:

1. Number of forms reviewed.
2. Number of forms requesting SSNs.
3. Number of SSN justifications accepted and not accepted.
4. Identification of forms where SSNs were not allowed.
5. Identification of forms where SSN was masked or truncated.

(b) For DoD Component forms, the Components shall maintain a similar database as the DoD Forms Management Officer and produce the same report every July 1 for inclusion in the annual report required by section 3544(c) of Reference (l). Exceptions to this requirement can be approved by the DPCLC.

(c) For command and installation forms, no reporting shall be required with the exception of annual reporting on July 1 of specific instances in which SSN use on forms has not

been accepted. In the case where a DoD Component maintains command and installation data, it can also be reported in its annual report.

(2) Existing Forms

(a) For DD and SD forms, the DoD Forms Management Officer shall report the results of the review for existing forms and the periodic reviews for input into the FISMA Report. This report shall include:

1. Total number of forms in the database.
2. Number of forms containing SSNs.
3. Number of forms reviewed.
4. Number of forms where SSN justifications were accepted.
5. Number of forms where SSN justifications were not accepted.
6. Identification of forms where SSN justification was accepted.
7. Identification of forms where SSN was masked or truncated.

(b) The DoD Components shall provide the same information as the DoD Forms Management Officer for their Components as input into the FISMA Report. Exceptions to this requirement can be approved by the DPCLO.

(c) At the command and installation levels no reports are required, with the exception of specific examples where SSNs were eliminated or better masked, unless the DoD Component collects data at this level.

c. Schedule. Annually, on July 1, produce all data and reports related to new and existing forms at all levels.

2. DoD SYSTEMS

a. DITPR

(1) The DITPR is a key tool in the plan to reduce SSN use in DoD systems.

(2) All data elements in the DITPR relating to SSNs are mandatory data fields and shall be completely filled out by all DoD Components.

(3) All automated systems containing SSNs shall be included in the DITPR in accordance with “DoD IT Portfolio Repository (DITPR) and DoD SIPRNET IT Registry Guidance 2007-2008” (Reference (m)).

(4) All systems in DITPR shall report:

(a) Whether the system (or initiative) contains SSNs (full or truncated) or uses SSNs in the system.

(b) The justification for using SSNs. (This field should be consistent with the categories of acceptable use of SSNs in Enclosure 2 and specific legislative requirements.)

b. DPCLO System Review Report Process. The initial SSN use case justifications are to be included in the DoD Component report to the DPCLO as a part of the annual FISMA submission using the process detailed in subparagraphs 2.b.(1) through 2.b.(3)(e) of this enclosure. Thereafter, DPCLO shall submit a report annually for input into the Privacy section of the annual FISMA Report, as part of the biennial Privacy Act SORN review. Since this review is on a biennial review schedule, the DPCLO shall produce a biennial schedule for the system reviews. Exceptions to this requirement can be approved by the DPCLO. The review and reporting process is as follows:

(1) The Component official approves SSN justification; this process is further detailed in section 3 of Enclosure 4 and section 3 of Enclosure 5.

(2) DPCLO reviews and approves or disapproves SSN justifications as an extension of the biennial Privacy Act SORN review. Where a justification for SSN use is not accepted, the action officer will prepare a plan, to include milestones and a timeline, for the elimination of SSN usage; this process is further detailed in section 4 of Enclosure 4. The final date for SSN elimination will be provided by the DoD Component to the DPCLO.

(3) DPCLO prepares its annual report in accordance with the annual FISMA schedule. This report shall include the following elements and any new elements as required:

(a) Total number of information technology (IT) systems in DITPR.

(b) Total number of IT systems with SSNs.

(c) Total number of IT systems with SSNs reviewed.

(d) Total number of IT systems with SSNs approved and disapproved.

(e) Identification of IT systems with SSNs disapproved.

3. IG, DoD REVIEW. The IG, DoD and the Service audit agencies shall review the implementation of the DoD SSN Use Reduction Plan at key milestones as reflected in this

Instruction. The internal controls established in the DoD SSN Use Reduction Plan may be considered for review as “Command Interest Items.” The following issues shall be addressed:

- a. Whether every organizational level followed the procedures required in the SSN Use Reduction Plan.
- b. Whether there are SSN justifications for forms and systems.
- c. Whether Heads of DoD Components are reviewing and approving SSN justifications.
- d. Whether actual reported results are accurate.

ENCLOSURE 4

APPROVAL FOR USE OF THE SSN

1. ACCEPTABLE USES

- a. The general list of acceptable uses of the SSN is in Enclosure 2.
- b. Justification for the use of the SSN may also be found in the appropriate SORN or PIA.

2. DOCUMENTATION

a. DITPR

(1) The DITPR requires all DoD information systems to state whether or not the system collects SSNs.

(2) Acceptable justification shall be annotated in the appropriate DITPR field.

(3) In cases where the justification is "Other Uses," appropriate explanation of the supporting legal authority and the particular use case shall be entered into the Comment field.

(4) Where continued use of the SSN is not accepted by the DPCCLO, system managers shall work with their DoD Component privacy offices to develop a plan for the removal of the SSN. This plan shall be maintained by the action officer.

(5) The justification for SSN usage in new information system development must be approved during the design and approval processes prior to initiation of system implementation.

b. Forms

(1) Requesting the use of SSNs will be part of the forms approval process, including the use of DD Form 67.

(2) Requesting the use of SSNs shall include the supporting documentation described in section 1 of Enclosure 3.

(3) Reviewing of all forms shall be completed in accordance with DoD Instruction 7750.07 (Reference (n)).

3. DoD COMPONENT CONCURRENCE

a. DoD Component concurrence for the use of the SSN shall be documented in a memorandum for DPCLCLO. Figure 1 of this enclosure contains a sample memorandum.

b. The memorandum shall include:

(1) Name of the DoD information system or name and number of the form that will collect, use, maintain, and/or disclose the SSN.

(2) Specific use case that grants authority for use of the SSN.

(3) Citation of statutory requirement for the use of the SSN, if applicable.

(4) Appropriate system or form supporting documentation (e.g., SORN).

(5) Physical, technical, and administrative safeguards to be put in place to reduce exposure of the SSN.

(6) If continued use of the SSN is not justified by one of the 13 acceptable use cases specified in section 2 of Enclosure 2, a plan to eliminate the use of the SSN as described in section 4 is required.

(7) An explanation of why any alternatives to the SSN that were considered are unacceptable (this is only required when legacy system interface is selected as the specific use case that grants authority for use of the SSN).

Figure 1. Sample SSN Justification Memorandum

(Month, Day, Year)

MEMORANDUM FOR DEFENSE PRIVACY AND CIVIL LIBERTIES OFFICE

SUBJECT: Justification for the Use of the Social Security Number (SSN) – [Form or System Name/Number]

The memorandum should begin by naming and describing the system or form that is the subject of the justification. The description should be sufficiently detailed so that someone unfamiliar with the system should be able to grasp a general understanding of its intent.

The justification for the use of the SSN should include a reference to the SSN instruction use case that is being used to justify the use of the SSN. If the justification does not fall under either the operational necessity use case or the legacy system interface use case, then the justification shall also include the specific legal authority that requires the use of the SSN and why it is applicable to the use being justified.

Reference should be made to the system or form supporting documentation, including, but not limited to, SORN, PIA, collection in accordance with sections 3501-3520 of Reference (1), also known as the “Paperwork Reduction Act,” or any other documentation that may be appropriate. If the substance of the documentation is not attached, reference should be made to how the reader may gain access to this documentation.

Justification for the use of the SSN does not constitute blanket permission to use the SSN. Specific reference shall be made to indicate actions being taken to reduce the vulnerability of SSNs, which may include indicating where SSNs are being removed from transactions or any other protections that have been included. It should be obvious to the reader that a thorough effort has been made to evaluate the risk associated with the system or form and that every reasonable step has been or is being taken to reduce the use of the SSN and protect it where the use is still required.

If the justification for the use of the SSN falls under the legacy use case and is not specifically required by the law, reference shall be made to the Plan of Actions and Milestones for the elimination of the use of the SSN and that plan shall be attached.

Official’s Name
Title

4. PLAN TO ELIMINATE USE OF THE SSN

a. Any use of the SSN that cannot be justified through appropriate authorities must be eliminated.

b. Elimination of the use of the SSN shall be completed consistent with the existing life cycle to reduce impact on operations and decrease overall cost.

c. The plan to eliminate the use of the SSN shall include:

(1) The alternative being used to replace the function for which SSNs have been used.

(2) Associated forms and systems that will be affected by elimination of the SSN.

(3) A mitigation strategy to reduce or eliminate the effects of removal of the SSN in conjunction with associated forms or systems.

(4) Timeline, with milestones, for removal of the SSN.

(5) Where elimination is not to occur immediately, include interim measures to provide additional protection of the SSN.

(6) Where elimination is dependent on changes to other systems and/or forms, include efforts made to work with owners of those systems and/or forms to collaborate and eliminate the use of SSNs.

d. An example of an elimination plan can be seen in Figure 2 of this enclosure.

Figure 2. Sample SSN Elimination Plan

Sample SSN Elimination Plan
System/Form Name: _____
System of Records Notice Number: _____
System/Form Owner: _____
Inputs that use, provide, or are identified by SSN:
Forms: DD Form XXX – For each form the plan shall include the purpose that the SSN serves as well as potential alternatives. Some level of detail shall be included regarding the owner of the form and any pertinent details regarding the form owner’s plan to eliminate the use of the SSN.
Systems: XXX System – For each system that provides an input to a system or is responsible for generating the form, the plan shall discuss the purpose served by the SSN and any potential alternatives. Some level of detail shall be included regarding the system owner and any important details regarding their plan to eliminate the use of the SSN.
Outputs that include or are identified by the SSN:
Forms: DD Form XXX – For each form the plan shall include the purpose that the SSN serves as well as potential alternatives. Some level of detail shall be included regarding the owner of the form and any pertinent details regarding the form owner’s plan to eliminate the use of the SSN.
System: XXX System – For each system that provides an input to the system or is responsible for generating the form, the plan shall discuss the purpose served by the SSN and any potential alternatives. Some level of detail shall be included regarding the system owner and any important details regarding their plan to eliminate the use of the SSN.
Elimination Strategy and Timeline:
The strategy shall include specific steps that must be accomplished to eliminate the use of the SSN with dates by which these steps will be accomplished. Be sure to include all appropriate references to dependencies such as other forms or systems, availability of resources (manpower, funding, etc) and dates by which these milestones will be completed.
While it is clear that there may be significant constraints on making these changes, it is not acceptable to avoid activity through mutual dependencies.
Interim Strategy and Timeline:
Where elimination of the SSN cannot be achieved quickly or directly, interim steps shall be taken to provide better protection for SSNs. This may include masking or truncation, changes to displays or reports, or any other steps that can be shown to provide improvements to protection.

ENCLOSURE 5

RESPONSIBILITIES

1. USD(P&R). The USD(P&R) shall establish and oversee the implementation of DoD policy concerning the reduction of SSN use within DoD.

2. DIRECTOR OF ADMINISTRATION AND MANAGEMENT (DA&M). The DA&M shall ensure that the DoD Forms Management Officer and the Director, DPCLCLO, implement the SSN Use Reduction Plan as described in this Instruction.
 - a. DoD Forms Management Officer. The DoD Forms Management Officer shall review SSN use and justifications on new and existing DD and SD forms and produce an annual report on results.

 - b. Director, DPCLCLO. The Director, DPCLCLO, shall:
 - (1) Provide the final approval authority for SSN use and justification. The authorization for use of PII is governed through the DoD Privacy Program in accordance with References (j) and (k).

 - (2) Review SSN use and justifications in the DITPR, in accordance with the guidance in Reference (m), as part of the biennial Privacy Act SORN review, required by the Defense Privacy Program, and prepare an annual report on results as described in Enclosure 3.

 - (3) Submit the annual report required by section 3544(c) of Reference (l). This report requires agencies to review and update their progress on the reduction of holdings of PII. Provide specific guidance annually to reflect the reporting elements. FISMA elements are subject to change. The DoD Component Privacy offices are responsible for providing input to the DPCLCLO for inclusion in the report.

 - (4) Establish detailed guidance and additional reports as necessary to support DoD efforts in SSN collection, use, dissemination, and reduction.

3. IG, DoD. The IG, DoD, in addition to the responsibilities in section 4 of this enclosure, shall review the implementation of the DoD SSN Use Reduction Plan at the key milestones reflected in Enclosure 3.

4. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall conduct periodic reviews of SSN use. The results of the review and justifications for all forms and systems shall be included in an annual report prepared in accordance with the process described in Enclosure 4. Reports shall be forwarded to the Director, DPCLO.

5. COMMANDERS OF THE COMBATANT COMMANDS. The Commanders of the Combatant Commands, in addition to the responsibilities in section 4 of this enclosure, through the Chairman of the Joint Chiefs of Staff, shall review and approve uses of the SSN that are required as a result of operational necessity.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

DA&M	Director of Administration and Management
DEERS	Defense Enrollment Eligibility Reporting Systems
DITPR	DoD Information Technology Portfolio Repository
DMDC	Defense Manpower Data Center
DPCLO	Defense Privacy and Civil Liberties Office
EDI-PI	Electronic Data Interchange Personal Identifier
E.O.	Executive Order
FISMA	Federal Information Security Management Act
IG, DoD IT	Inspector General of the Department of Defense information technology
MOU	memorandum of understanding
NCIC	National Crime Information Center
NEO	Noncombatant Evacuation Operations
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
PIA	Privacy Impact Assessment
PII	personally identifiable information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RCS	Report Control Symbol
SORN	System of Records Notice
SSN	Social Security Number

USD(P&R) Under Secretary of Defense for Personnel and Readiness

PART II. DEFINITIONS

These terms and their definitions are for the purpose of this Instruction.

application. Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. Examples include office automation, electronic mail, Web services, and major functional or mission software programs.

authentication. The process of establishing that an individual, previously identified and with whom a business relationship has been established, is the same as the individual who initially created the relationship. This is generally done by presenting information that is known only to the individual and the organization. Authentication is also a security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

computer network. The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities such as local or campus area networks, or long-haul data transport capabilities such as operational, metropolitan, or wide area and backbone networks.

DoD Forms Management Officer. The individual who is responsible for forms management for the Department of Defense. Specifically, the individual who is responsible for all DD and SD forms.

DoD Information System. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

electronic form. An officially prescribed set of data residing in an electronic medium that is used to produce as near to a mirror-like image of the officially prescribed form as the creation software will allow. An electronic form can also be one in which prescribed fields for collecting data can be integrated, managed, processed, and/or transmitted through an organization's IT system. There are two types of electronic forms: one that is part of an automated transaction, and one whose image and/or data elements reside on a computer.

form. A fixed arrangement of captioned spaces designed for entering and extracting prescribed information. Forms may be preprinted paper forms or electronic forms.

identification. The act of establishing who a person is. This is generally done by the collection and review of certain identity attributes, including, but not limited to, name, SSN, address, and

date of birth. Identification is generally associated with a business process and includes establishing the relationship based on the need or desire of an individual to participate in the given business process.

personal information. Information about an individual that identifies, links, relates, or is unique to, or describes him or her (e.g., SSN, age, military rank, civilian grade, marital status, race, salary, home or office phone numbers, or other demographic and biometric personnel, medical, and financial information). Such information is also known as PII (i.e., information that can be used to distinguish or trace an individual's identity, such as his or her name, SSN, date and place of birth, mother's maiden name, and biometric records, including any other personal information that is linked or linkable to a specified individual).

PIA. An analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of collecting, maintaining, and disseminating PII information in an electronic information system; and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic), about an individual that is maintained, including, but not limited to, his or her education, financial transactions, medical history, criminal or employment history, and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, a voice print, or a photograph.

SORN. A public notice detailing the conditions, contents, and procedures for a system of records, including system identifications, system locations, categories of records and individuals contained in the system, access procedures, and legal exemptions. SORNs must be published in accordance with Reference (j).

system. See DoD Information System.

system identifiers. Identifiers used for system-to-system electronic communications across the enterprise. They are not to be declared by, nor in fact generally known to, the person they are assigned to. Their primary purpose is to limit the ambiguity in identity caused by human entry of declarative identifiers (e.g., transpositions and typographical errors that occur when entering SSNs). Once they are assigned they are used only for technology-to-technology communications and never printed on any media. Their scope is only for use within the Department of Defense.

system of records. A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.