UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, DC 20301-4000

PERSONNEL AND
READINESS

MAR 28 2008

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Directive-Type Memorandum (DTM) 07-015-USD(P&R) – "DoD Social Security Number (SSN) Reduction Plan"

References:
(a) President's Task Force on Identity Theft Strategic Plan, April 2007[1]
(b) DoD Senior Privacy Official Memorandum, "Personally Identifiable Information," April 27, 2007[2]
(c) 5 U.S.C 552a
(d) Executive Order 9397, "Numbering System for Federal Accounts Relating to Individual Persons," November 22, 1943
(e) DoD 5400.11-R, "DoD Privacy Program," May 14, 2007
(f) Subchapter III, chapter 35 of title 44, United States Code
(g) CIO/NII DoD Information Technology (IT) Portfolio Repository and DoD SIPRNET IT Registry Guidance, 2007-2008[3]

Purpose. This DTM establishes the DoD policy for the use of the SSN and guidance for reducing its unnecessary use. Reference (a) requires all Federal agencies to develop and implement a plan to reduce the unnecessary use of SSNs. This Plan must be developed by April 2008 per Reference (b). This DTM is effective immediately; it shall be converted to a DoD Instruction within 180 days.

Applicability. This DTM covers all uses of SSNs within DoD, to include DoD data managed or retained in contractor-owned, -managed or -operated systems (Reference (c)).

[1] Copies of document are available at: www.idtheft.gov/reports/strategicplan.pdf
[2] Copies of document are available at: DoD Defense Privacy Office, 703-607-2943
[3] Copies of document are available at: DoD CIO (IT Policy), 703-601-4729

Policy. It is DoD policy to reduce or eliminate the use of SSNs wherever possible. Attachment 1 contains the guidance for the appropriate use of SSNs within the Department of Defense. Attachment 2 is the DoD SSN Reduction Plan. Definitions are provided at Attachment 3.

Responsibilities

- 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 (Attachment 2).

- The DoD Component Forms Management Officers shall review SSN use and justifications for new and existing Component-wide forms and produce an annual report on results. New and existing command and installation level forms also will be reviewed with limited reporting (Attachment 2).

- The DoD Senior Privacy Official shall review SSN use and justifications on the DoD Information Technology Portfolio Repository as part of the Biennial Personally Identifiable Information Review Process and prepare an annual report on results (Attachment 2).

- The DoD Inspector General (IG) is requested to review the implementation of the DoD SSN Reduction Plan (Attachment 2).

Releasability. UNLIMITED. This memorandum is approved for public release. Copies may be obtained through the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

David S. C. Chu

David S. C. Chu

Attachments:
As stated

ATTACHMENT 1

GUIDANCE ON THE USE OF THE SSN BY THE DEPARTMENT OF DEFENSE

1. OVERVIEW

a. The SSN has been used as a means to efficiently identify and authenticate individuals. Expanded use of the SSN has increased efficiency, enabling systems and processes to interoperate and transfer information with a greatly reduced chance of errors. The threat of identity theft has rendered this wide-spread use unacceptable, requiring all Federal agencies to evaluate how the SSN is used and eliminate its unnecessary use (Reference (a)).

b. This guidance identifies the acceptable uses of the SSN, describes how authorized uses shall be documented, presents alternatives to using the SSN, and explains the role Personally Identifiable Information (PII) training plays in protecting privacy information within the Department of Defense. Any uses of the SSN not provided for in this guidance 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, 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 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 use of the SSN shall be limited to transactions that specifically require the presentation of the SSN to meet a statutory or regulatory requirement. Most applications that require the SSN for specific transactions do not require its use for every transaction. For example, systems that link to financial institutions may need the SSN for initial interactions, but thereafter use an account number or some other form of identification or authentication. As such there is no need to use the SSN for individuals to authenticate themselves as part of every transaction.

c. Executive Order 9397 (Reference (d)) authorized all Federal agencies to use the SSN as a primary means of identification for individuals working for, with, or conducting business with the agency. The blanket use of the SSN as provided by Reference (d) is in the process of being partially rescinded by the Office of Management and Budget (OMB) and they will not accept its citation no longer will accept its citation as sufficient justification for the use of the SSN. What follows are general categories of use that may continue to be acceptable for the SSN. General coverage of an application by one of the following use cases 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 of use of the SSN in every transaction or interaction. Any transaction that includes 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 Armed Forces of the United States. Many of the systems, processes, and forms used by the Department of Defense categorize individuals by their SSNs. In many cases, it is essential to be able to identify individuals for the purpose of the Geneva Convention. In addition, it may be necessary to access this number at short notice.

(2) Law Enforcement, National Security, Credentialing. Almost every law enforcement application must be able to report and track individuals 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, or verification of 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. Federal law requires that individuals who hold accounts with financial institutions must provide the SSN as part of the process to open accounts. It may therefore be required for systems, processes, or forms that interface with or act on behalf of individuals or organizations in transactions with financial institutions to provide the SSN.

(5) Confirmation of Employment Eligibility. Federal statute requires that all persons employed within the United States must provide an SSN or comparable identifier to prove that he or she is eligible to work for or with the government of the United States. Any system that deals with employment eligibility must contain the SSN.

(6) Administration of Federal Worker's Compensation. The Federal Worker's 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 must contain the SSN. Additionally, individuals who operate business vehicles 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 should be rigorously scrutinized to determine the availability of some other means of 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 3.b.(1) through 3.b.(10) for the continued use of the SSN may not be able to transition to another identifier in a timely manner 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 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 of the application.

(12) Other Cases. The previous categories may not include all uses of the SSN delineated 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.(10) of this Attachment is required by law, then 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 under this justification.

3. DOCUMENTING AUTHORIZED USES

a. Any system, process, or form that collects, transfers, or retains 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 the DoD Privacy Program. 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 the specific legislative requirement for the 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. Uses of PII that are not properly documented may be in violation of Federal law.

Individuals who choose to use PII without proper documentation may subsequently be held accountable and face consequences provided for in Federal law.

b. Forms used to collect PII shall be coordinated with the DoD Component's Privacy Act Officer. The DD Form 67, "Forms 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 Privacy Act Officer and the systems of records number entered. Copies of the justification to collect PII and systems of records notice are included with the DD Form 67.

c. Documentation for this justification shall be retained and available upon request.

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. Alternatives include:

a. Electronic Data Interchange – Personal Identifier (EDI-PI)

(1) The EDI-PI is a unique system identifier that is used for machine-to-machine transactions by the Department of Defense. In the Defense Enrollment Eligibility Reporting System, the central repository for DoD person data, the EDI-PI is used as the primary identifier for all individuals. It is not a number that is known to the individuals, and it is never intended that the EDI-PI be used outside of machine-to-machine transactions.

(2) The EDI-PI is the personal unique identifier used as part of the Cardholder Unique Identifier, which is part of the Homeland Security Presidential Directive-12 solution for the Department of Defense. As such, it may be used as an identifier when the Common Access Card is used to electronically authenticate an individual. A greater shift to electronic authentication would reduce the use of the SSN and provide greater security for transactions.

b. System-Specific Identifiers. In use cases that are linked to a limited number of other applications, the best opportunity may be to create a unique identifier for those uses. In particular, for situations in which members of the public are required to gain access, particularly on a temporary basis, this may solve 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 applications that are finite in scope and 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" (as opposed to "something one has" (e.g., a CAC with PKI certificates) and "something one knows" (e.g., a PIN)), 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.)

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. To ensure that all personnel are so trained, DoD 5400.11-R (Reference (e)) requires that, prior to operating systems that contain or use PII, individuals be trained on their appropriate handling. In addition to this use-specific training, Reference (e) 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.

ATTACHMENT 2

DoD SSN REDUCTION PLAN

1. INTRODUCTION. This Reduction Plan covers all uses of SSNs within the Department of Defense, to include DoD data managed or retained in contractor-owned, -managed or -operated systems, to include all requirements of Reference (e). This plan focuses on SSN use in DoD forms and systems, but the acceptable uses of SSNs in Attachment 1 apply to any use of SSNs including, but not limited to, surveys, spreadsheets, and hard copy lists. SSN use outside of approved forms and systems will be eliminated. This DTM will be followed by a DoD Instruction where additional guidance will be included.

2. DOD FORMS

a. Use of SSN on DoD Forms

(1) New Forms:

(a) Action Officer Requirements

1. Provide justification for using SSNs. (See Attachment 1 for acceptable uses.)

2. If justified, indicate if the SSN can be truncated or masked.

3. Relate the form to a system of records, privacy impact assessment, and the DoD Information Technology Portfolio Repository (DITPR) ID number, as applicable.

(b) Signing SSN Justifications. Senior Executive Service (SES) rank individual or a flag officer signature is required.

(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 Component DoD privacy officials.

2. For DoD Component-wide forms, the justifications shall be reviewed by the Component forms management officer, who shall consult with the Component privacy official.

3. For command and installation forms, the justifications shall be reviewed at least one administrative level above the senior signing official.

(2) Existing Forms:

(a) One-Time 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 Attachment 1.

2. The DoD Component-wide forms management officers shall conduct reviews of all Component forms to ensure compliance with the guidance in Attachment 1.

3. For command and installation forms, the appropriate forms management officers shall conduct reviews to ensure compliance with the guidance in Attachment 1.

4. Where a justification for SSN use is rejected the action officer will prepare a plan, to include milestones and a timeline, for the elimination of SSN usage.

(b) Periodic Review of SSN Use and Justification. SSN use and justification review shall be an added feature of the current periodic review process for all forms. This periodic review should be no less frequent than the systems of records review and may be tied to the systems of records notice review every 3 years.

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 every July 1. This report shall be an input into the Privacy section of the annual Federal Information System Management Act (FISMA) Report as required by subchapter III, chapter 35 of title 44, United States Code (Reference (f)). The annual report shall contain the following elements:

1. Number of forms reviewed.

2. Number of forms requesting SSNs.

3. Number of SSN justifications accepted and rejected.

4. Examples of forms where SSNs were not allowed.

5. Examples of SSN masking or truncation.

(b) For DoD Component-wide forms, the Components' forms management officers shall maintain a similar database as the DoD Forms Management Officer and produce the same report for their Components every July 1 for inclusion into the Privacy section of the annual FISMA Report.

(c) For command and installation forms, no database shall be required with the exception of annual reporting on July 1 on success stories for forms where SSNs were requested

but rejected. In the case where a DoD Component does maintain 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 both the one-time initial review of existing forms and the periodic reviews for input into the FISMA Report. This report shall include the following elements:

1. Total number of forms in the database.

2. Number of forms reviewed.

3. Number of forms containing SSNs.

4. Number of forms where justifications were questioned.

5. Number of SSN justifications accepted and rejected.

6. Examples of forms where SSNs were not allowed.

7. Examples of SSN masking or truncation.

(b) The DoD Component forms management officers shall provide the same information as the DoD Forms Management Officer for their Components.

(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

(1) July 1, 2008. Annually produce all data and reports related to new forms at all levels.

(2) July 1, 2009. Add all data and reports related to existing forms at all levels.

3. 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 according to the CIO/NII DoD IT Portfolio Repository and DoD SIPRNET IT Registry Guidance, 2007-2008 (Reference (g)).

(4) Two new fields were added in October 2007 that will become fully operational in March 2008:

(a) Does this system (or initiative) contain SSNs (full or truncated) or use SSNs in the system?

(b) What is the legal justification for using SSNs? (This field should be consistent with the categories of acceptable use of SSNs in Attachment 1.)

(5) As part of the SSN Reduction Plan, one additional field shall be added to DITPR in 2008: "What DoD forms are inputs (or outputs) to the system, including OMB control numbers, if applicable?" In 2008, this only applies to systems that contain SSNs.

b. SSNs in Systems Report Review Process. The initial SSNs in Systems Report, prepared by the Defense Privacy Office (DPO) using the process detailed in subparagraphs 2.b.(1) through 2.b.(3)(e), shall be due July 1, 2008. Thereafter, DPO shall submit a report annually by July 1 for input into the Privacy section of the annual FISMA Report, as part of the larger PII review process. Since the PII review process is on a biennial review schedule, the DPO shall produce a schedule for the system reviews. The review and reporting process is as follows:

(1) Systems senior official (flag officer or SES equivalent) signs off on SSN justification.

(2) DPO reviews SSN justifications as an extension of the biennial PII review process. Where a justification for SSN use is rejected the action officer will prepare a plan, to include milestones and a timeline, for the elimination of SSN usage.

(3) DPO prepares its annual report. The report shall include:

(a) Total number of 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) Examples of IT systems disapproved.

4. IG REVIEW

a. The DoD IG and the Service audit agencies are requested to review the implementation of the DoD SSN Reduction Plan. The new internal controls established in the DoD SSN Reduction Plan may be considered for review as "Command Interest Items."

b. For DoD systems, the following issues are requested to be reviewed:

(1) Are all IT systems with SSNs being registered in DITPR?

(2) Are there SSN justifications for systems in DITPR?

(3) Are there senior reviews of SSN justifications?

(4) Have the actual reported results been accurate?

c. For DoD forms, the following issues are requested to be reviewed:

(1) Has every organizational level followed the procedures required in the SSN Reduction Plan?

(2) Are there SSN justifications for forms?

(3) Are there senior reviews of SSN justifications?

(4) Have the actual reported results been accurate?

ATTACHMENT 3

DEFINITIONS

The following definitions only apply to this Directive-Type Memorandum.

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 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 as the creation software will allow of the officially prescribed form. 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.

privacy impact assessment. 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 personally identifiable 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 about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the name or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

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.