an inmate to accumulate vacation credit when:

(1) The inmate is transferred to another institution for the benefit of the government or because of the inmate's favorable adjustment (custody reduction); or

(2) The inmate is placed in a new work assignment in the institution for the benefit of the government or institution, rather than solely at the inmate's request or because of the inmate's poor performance or adverse behavior.

§ 545.28 Achievement awards.

Inmates may receive achievement awards in the following manner:

(a) *Education program completion.* With prior approval of the Education Department, each inmate who completes the Literacy program, Vocational Training, or related trades classroom work that is part of a certified apprenticeship program may be granted an achievement award from performance pay funds.

(b) *Drug treatment satisfactory progress/completion.* With prior approval of the Psychology Services Department, each inmate who is making satisfactory progress or completes a residential drug treatment program may also be granted an achievement award from performance pay funds.

§ 545.29 Special awards.

Inmates who perform exceptional services not ordinarily a part of the inmate's regular assignment may be granted a special award regardless of the inmate's work or program status. The special award may be in the form of a monetary payment in addition to any other award (e.g., extra good time) given.

§ 545.30 Funds due deceased inmates.

If performance pay is due to a deceased inmate for work performed and not yet paid, the Bureau will make the payment to a legal representative of the inmate's estate or in accordance with the laws of descent and distribution of the state of domicile (most recent legal residence).

[FR Doc. 2010–3902 Filed 3–2–10; 8:45 am]

BILLING CODE 4410–05–P

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 157

[DoD–2008–OS–0075; RIN 0790–AI33]

Reduction of Use of Social Security Numbers (SSN) in the Department of Defense (DoD)

AGENCY: Department of Defense.

ACTION: Proposed rule.

SUMMARY: This proposed rule establishes policy and assigns responsibilities for social security number (SSN) reduction in DoD. It incorporates Office of the Under Secretary of Defense for Personnel and Readiness Directive-type Memorandum titled "DoD Social Security Number (SSN) Reduction Plan."

DATES: Comments must be received by May 3, 2010.

ADDRESSES: You may submit comments, identified by docket number and/or the Regulatory Information Number (RIN) number and title, by any of the following methods:

- *Federal Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Mail:* Federal Docket Management System Office, 1160 Defense Pentagon, Washington, DC 20301–1160.

Instructions: All submissions received must include the agency name and docket number or RIN for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at *http://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Andrew Uscher, 703–696–0109.

SUPPLEMENTARY INFORMATION:

Executive Order 12866, "Regulatory Planning and Review"

It has been certified that 32 CFR part 157 does not:

(1) Have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy; a section of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribunal governments or communities;

(2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency;

(3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or

(4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in this Executive Order.

Section 202, Public Law 104–4, "Unfunded Mandates Reform Act"

It has been certified that 32 CFR part 157 does not contain a Federal mandate that may result in the expenditure by State, local and tribunal governments, in aggregate, or by the private sector, of $100 million or more in any 1 year.

Public Law 96–354, "Regulatory Flexibility Act" (5 U.S.C. 601)

It has been certified that 32 CFR part 157 is not subject to the Regulatory Flexibility Act (5 U.S.C. 601) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities. This rule establishes policy and assigns responsibilities for SSN reduction in DoD.

Public Law 96–511, "Paperwork Reduction Act" (44 U.S.C. Chapter 35)

It has been certified that 32 CFR part 157 does not impose reporting or recordkeeping requirements under the Paperwork Reduction Act of 1995.

Executive Order 13132, "Federalism"

It has been certified that 32 CFR part 157 does not have federalism implications, as set forth in Executive Order 13132. This rule does not have substantial direct effects on:

(1) The States;

(2) The relationship between the National Government and the States; or

(3) The distribution of power and responsibilities among the various levels of Government.

List of Subjects in 32 CFR Part 157

Privacy, Security measures, Social Security numbers.

Accordingly, 32 CFR part 157 is proposed to be added to read as follows:

PART 157—REDUCTION OF USE OF SOCIAL SECURITY NUMBERS (SSN) IN THE DEPARTMENT OF DEFENSE (DOD)

Sec.

157.1 Purpose.
157.2 Applicability.
157.3 Definitions.
157.4 Policy.
157.5 Responsibilities.
157.6. Guidance on the use of the SSN by the DoD.
157.7. DoD SSN reduction in forms and systems.
157.8. Approval for use of the SSN.
157.9 Information requirements.

Appendix A to Part 157—Sample SSN Justification Memorandum
Appendix B to Part 157—Sample SSN Elimination Plan

Authority: 5 U.S.C. 301.

§ 157.1 Purpose.

This part establishes policy and assign responsibilities for social security number (SSN) reduction in the Department of Defense (DoD). It establishes a DoD SSN Reduction Plan.

§ 157.2 Applicability.

This part:

(a) Applies to the Office of the Secretary of Defense, 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 DoD (hereafter referred to collectively as the "DoD Components").

(b) Covers all uses of SSNs within DoD, to include DoD data managed or retained in contractor-owned, -managed, or -operated systems according to section 552a of title 5, United States Code.

§ 157.3 Definitions.

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

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 information technology (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 (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 Personally Identifiable Information (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. All books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the information value of the data in them.

Survey. An instrument designed to gather data or attitudes by polling a section of the population.

System. See definition of 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 DoD.

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.

§ 157.4 Policy.

It is DoD policy that:

(a) All DoD personnel and contractors 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 will not be used in surveys, spreadsheets, or hard copy lists. The policy that SSNs will not be used in surveys only includes survey responses.

(d) SSNs will be used only in approved forms and systems when they meet one or more of the acceptable use criteria in § 157.6(b) of this part.

(e) Specific reviews of forms and systems will be conducted to reduce SSN use. Follow guidance in § 157.7 and § 157.8 of this part.

§ 157.5 Responsibilities.

(a) The Under Secretary of Defense for Personnel and Readiness (USD (P&R)) shall establish a SSN Reduction Plan for DoD and shall monitor its execution.

(b) The Director of Administration and Management shall ensure that the DoD Forms Management Officer and the Director, Defense Privacy Office (DPO) fulfill their responsibilities related to the SSN Reduction Plan.

(1) The DoD Forms Management Officer shall review SSN use and justifications on new and existing Department of Defense (DD) and Secretary of Defense (SD) forms and produce an annual report on results.

(2) The Director, DPO, shall:

(i) Provide the final approval authority for SSN use and justification. The authorization for use of personally identifiable information (PII) is governed through the DoD Privacy Program.

(ii) Review SSN use and justifications on the DoD Information Technology Portfolio Repository (DITPR) as part of the Biennial Privacy Act System of Records Notices Review and prepare an annual report on results (see § 157.7(b)(2)(iii) of this part).

(iii) Submit the Privacy Section of the annual Federal Information Security Management Act (FISMA) Report. 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 Act offices are responsible for providing input to the Defense Privacy Office for inclusion in the report.

(c) The Heads of the DoD Components shall review, or delegate responsibility for review within their Component SSN use and justifications for new and existing Component-wide forms, and produce an annual report on results in accordance with the process described in § 157.8(b)(2)(i) of this part. New and existing command and installation level forms also will be reviewed with limited reporting in accordance with the process described in § 157.8(b)(2)(ii) of this part.

(d) The Commanders of the Combatant Commands, 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.

(e) The IG, DoD, is requested to review the implementation of the DoD SSN Reduction Plan at key milestones as reflected in § 157.7(c) of this part.

§ 157.6 Guidance on the use of the SSN by DoD.

(a) *Overview.* (1) The SSN has been used as a means to efficiently 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 (President's Task Force on Identity Theft Strategic Plan [1] and Office of Management and Budget (OMB) Memo M–07–16 [2]).

(2) 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 Privacy Act training plays in protecting privacy information within DoD. 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 (last four digits), masked, partially masked, encrypted, or disguised SSNs.

(b) *Acceptable uses.* (1) The acceptable uses of the SSN are those that are provided for by law, require interoperability with organizations beyond DoD, 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.

(2) Executive Order 9397 required all federal agencies to use the SSN as a primary means of identification for individuals working for, with, or conducting business with their agency. The requirement for the use of the SSN provided by Executive Order 9397 has been eliminated. Executive Order 9397 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 constitute justification for ongoing use of the SSN.

(3) 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 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.

(i) *Geneva Conventions serial number.* As of the late 1960s, the SSN has served as the Geneva Conventions serial number for the Armed Forces of the United States. Many of the systems, processes, and forms used by DoD categorize individuals by their SSNs. In many cases, it is essential to be able to identify individuals for the purpose of the Geneva Conventions. In addition, it may be necessary to access this number at short notice.

(ii) *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.

(iii) *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.

(iv) *Interactions with financial institutions.* Federal law requires that individuals who hold accounts with financial institutions 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.

(v) *Confirmation of employment eligibility.* Federal statute requires that all persons employed within the United States 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 may contain the SSN.

(vi) *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.

(vii) *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

[1] Available at *http://www.idtheft.gov/reports/strategicplan.pdf.*

[2] Available at *http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.*

business vehicles under their own name may use their SSN as the tax number for that business function.

(viii) *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.

(ix) *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.

(x) *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.

(xi) *Legacy system interface.* Many systems, processes, or forms that do not meet the criteria in paragraphs (b)(3)(i) through (b)(3)(x) of this section 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.

(xii) *Operational necessity.* It is not the intention of this part 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 supersede 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 our Service members and the Department should be strongly considered prior to granting approval using this category of justification.

(xiii) *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 paragraphs (b)(3)(i) through (b)(3)(x) of this section 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 provision.

(c) *Documenting authorized uses.* (1) 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 32 CFR part 310. 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 per paragraph (b)(3) of this section 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 record notice must exist or be established prior to its use per 32 CFR part 310. The Defense Privacy Office will work with the DoD Component privacy official to develop the notice and forward for publication in the Federal Register. Individuals who choose to use PII without proper documentation may be in violation of section 552a of title 5, Unites States Code and may be held accountable to the stated consequences.

(2) Forms used to collect PII shall be coordinated with the DoD Component's Privacy Act officer. The DD Form 67, "Forms Processing Action Request," [3] 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 system of records number entered. Copies of the justification to collect PII and systems of records notice are included with the DD Form 67.

(3) Documentation for this justification shall be retained and available upon request.

(d) *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 following list is not meant to be definitive. For assistance in situations which are not specified, contact the Defense Manpower Data Center (*acossntigerteam@osd.pentagon.mil*). Alternatives include:

(1) *Electronic Data Interchange—Personal Identifier (EDI–PI).*

(i) The EDI–PI is a unique system identifier that is used for machine-to-machine transactions by DoD. In the Defense Enrollment Eligibility Reporting System, the central repository for DoD personnel 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.

(ii) 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 [4] solution for DoD. As such, it may be used as an identifier when the CAC 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.

(2) *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.

(3) *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.

(4) *Elimination of identifier.* Many instances where the SSN is collected or used may be able to be eliminated. The

[3] Available at *http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd0067.pdf.*

[4] Available at *http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.*

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.

(5) *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.)

(6) *Situational elimination/protection.* As previously stated, authority to collect, maintain, or use the SSN does not constitute blanket approval to use the SSN throughout the business process. Every report, display, printout, and transaction shall be reviewed to determine the requirement for the use of the SSN. If there is not a requirement for the SSN at that point, an alternative shall be found or the use should be eliminated. If where there is a requirement, determine whether the use can be further protected through truncation or masking.

(e) *Training.* It is vital to DoD 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, 32 CFR part 310 requires that, prior to operating systems that contain or use PII, individuals be trained on appropriate handling. In addition to this use-specific training, 32 CFR part 310 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.

§ 157.7 DoD SSN reduction in forms and systems.

(a) *DoD Forms*—(1) *Use of SSN in DoD forms*—(i) *New forms*—(A) *Action Officer requirements.* (*1*) Provide justification for using SSNs. (See § 157.6(b) for acceptable uses.)

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

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

(B) *Signing SSN justifications.* Senior Executive Service (SES) grade official or a general flag officer or equivalent signature is required (see § 157.8(c) of this part).

(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 DPO.

(*2*) For DoD Component forms, the justifications shall be reviewed by the Component Forms Management Officer, who shall consult with the DoD Component privacy officials.

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

(ii) *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 § 157.6 of this part.

(*2*) The DoD Component Forms Management Officers shall conduct reviews of all Component forms to ensure compliance with the guidance in § 157.6 of this part.

(*3*) For command and installation forms, the appropriate forms management officers shall conduct reviews to ensure compliance with the guidance in § 157.6 of this part.

(*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 (see § 157.8(d) of this part). The final date for SSN elimination will be provided to the DoD Forms Management Officer.

(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 Biennial Privacy Act System of Records Review.

(2) *Reporting results*—(i) *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 an input into the Privacy section of the annual FISMA Report as required by subchapter III, chapter 35 of title 44, United States Code. 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*) Identify forms where SSNs were not allowed.

(*5*) Identify forms where SSN was masked or truncated.

(B) For DoD Component 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 maintains command and installation data, it can also be reported in its annual report.

(ii) *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*) Identify forms where SSNs were not allowed.

(*7*) Identify forms where SSN was masked or truncated.

(B) The DoD Component forms management officers shall provide the same information as the DoD Forms Management Officer for their Components as input into the FISMA Report.

(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.

(3) *Schedule.* Annually, on July 1, produce all data and reports related to new and existing forms at all levels.

(b) *DoD Systems*—(1) *DITPR.* (i) The DITPR is a key tool in the plan to reduce SSN use in DoD systems.

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

(iii) All automated systems containing SSNs shall be included in the DITPR according to the Chief Information

Officer/Network and Information Integration (CIO/NII) DoD IT Portfolio Repository and DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry Guidance, 2007–2008 [5].

(iv) Two new fields were added in October 2007:

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

(B) What is the justification for using SSNs? (This field should be consistent with the categories of acceptable use of SSNs in § 157.6(b) of this part and specific legislative requirements.)

(2) *SSNs in Systems Report review process.* The initial SSNs in Systems Report, prepared by the DPO using the process detailed in paragraphs (b)(2)(i) through (b)(2)(iii)(E) of this section, shall be due with DoD Privacy FISMA reporting requirements. Thereafter, DPO shall submit a report annually for input into the Privacy section of the annual FISMA Report, as part of the Biennial Privacy Act System of Records Review. Since this review is on a biennial review schedule, the DPO shall produce a biennial schedule for the system reviews. The review and reporting process is as follows:

(i) Systems senior official (general flag officer or SES equivalent) signs off on SSN justification (see § 157.8(c) of this part).

(ii) DPO reviews SSN justifications as an extension of the Biennial Privacy Act System of Records Notices Review. 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 (see § 157.8(d) of this part). The final date for SSN elimination will be provided by the DoD Component Privacy Officials to the DPO.

(iii) DPO prepares its annual report according to the annual FISMA schedule. This report shall include the following elements and include any new elements as required:

(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) Identification of IT systems disapproved.

(c) *IG review.* (1) The IG, DoD and the Service audit agencies are requested to review the implementation of the DoD SSN Reduction Plan at key milestones as reflected in this document. The new internal controls established in the DoD SSN Reduction Plan may be considered for review as "Command Interest Items."

(2) For DoD systems, the following issues are requested to be reviewed:

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

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

(iii) Are there senior reviews of SSN justifications?

(iv) Have the actual reported results been accurate?

(v) Are Privacy Act system of records reviews conducted quarterly to comply with the Biennial Privacy Act System of Records Notices Review?

(3) For DoD forms, the following issues are requested to be reviewed:

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

(ii) Are there SSN justifications for forms?

(iii) Are there senior reviews of SSN justifications?

(iv) Have the actual reported results been accurate?

§ 157.8 Approval for use of the SSN.

(a) *Acceptable uses.* (1) The general list of acceptable uses of the SSN is listed in § 157.6(b) of this part as well as specific legislative requirements.

(2) A guide to laws requiring the use of the SSN can be found on the DoD Privacy Office Web site (*http://www.defenselink.mil/privacy/*). This list is merely a guide and may not cover every law.

(3) Another place to locate legal authority that may provide acceptable justification for the use of the SSN may be found in the appropriate System of Records Notice or PIA.

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

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

(iii) 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.

(iv) Where continued use of the SSN is rejected by the DPO, a plan will be developed for the removal of the SSN and shall be maintained by the action officer.

(2) *Forms.* (i) Requesting the use of SSNs will be part of the forms approval process, including the use of DD Form 67.

(ii) Requesting the use of SSNs shall include supporting documentation described in paragraph (a) of this section.

(iii) Reviewing of all forms shall be completed in accordance with DoD Instruction 7750.07 [6].

(c) *SES or General Flag Officer concurrence.* (1) Senior official concurrence for the use of the SSN shall be documented in a Memorandum for the Record (MFR). (See Appendix A to this part.)

(2) The MFR shall include the following information:

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

(ii) Specific use case which grants authority for use of the SSN.

(iii) Citation of statutory requirement for the use of the SSN.

(iv) Appropriate system or form supporting documentation, i.e., System of Records Notice or Certification and Accreditation

(v) Security precautions to be taken to reduce exposure of SSN.

(vi) If continued use of the SSN is not justified by legislative requirement, a plan to eliminate the use of the SSN as described in paragraph (d) of this section.

(3) In cases where the justification for the use of SSNs is operational necessity, approval must be from the Combatant Commander. Because this use case is intended for tactical situations, the approval does not need to be documented with an official memorandum. The format of the approval should be consistent with mechanism available and documented as applicable.

(d) *Plan to eliminate use of the SSN.* (1) Any use of the SSN that cannot be justified through appropriate legal authorities must be eliminated.

(2) Elimination of the use of SSN should be completed consistent with the existing life cycle to reduce impact on operations and decrease overall cost.

(3) The plan to eliminate the use of the SSN shall include the following information.

(i) Alternative being used to replace function for which SSNs have been used.

(ii) Associated forms and systems which will be affected by elimination of SSN.

(iii) Mitigation strategy to reduce or eliminate affects of removal of SSN in conjunction with associated forms or systems.

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

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

[5] Copies of this document are may be obtained by contacting DoD CIO (IT Policy) at 703–601–4729.

[6] Available at *http://www.dtic.mil/whs/directives/corres/pdf/775007p.pdf.*

(vi) 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.

(4) An example of an Elimination Plan can be seen in Appendix B to this part.

§ 157.9 Reporting requirements.

The FISMA Report has been assigned Report Control Symbol (RCS) DD–NII (Q,A) 2296. The Privacy Act Program reporting requirements have been assigned RCS DD–DA&M(AR) 1379. These reporting requirements have been approved and assigned a RCS number in accordance with DoD 8910.1–M.[7]

BILLING CODE 5001–06–P

[7] Available at *http://www.dtic.mil/whs/directives/corres/pdf/891001m.pdf.*

Appendix A to Part 157—Sample SSN Justification Memorandum

Sample SSN Justification Memorandum

(Month Day, Year)

MEMORANDUM OR THE RECORD

SUBJECT: Justification for the Use of the Social Security Number (SSN)

The memo 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 Usage Instruction Use Case that is being used to justify the use of the SSN. This shall also include the specific reference to the law or Federal Regulation 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, System of Records Notice (SORN), Privacy Impact Assessment (PIA), Paperwork Reduction Act (PRA) notice, 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 SSN, which may include indicating where SSNs are being removed from transactions, SSNs are no longer displayed, or any other protections that have been included. It should be obvious to the reader that 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 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.

Senior Official's Name
Title

Attachments:
As Stated

Appendix B to Part 157—Sample SSN Elimination Plan

Sample SSN Elimination Plan

System/Form Name: _____

System of Record Notice Number: _____

System/Form Owner: _____

Inputs that use, provide, or are identified by SSN:

Forms:
Form DDXXX – For each form, the plan should include the purpose the SSN serves as well as potential alternatives. Some level of detail regarding the owner of the form and any pertinent details regarding the form owners plan to eliminate the use of the SSN.

Systems:
XXX System – For each system that provides an input to the system or is responsible for generating the form, the plan should discuss the purpose served by the SSN and any potential alternatives. Some level of detail should 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 SSN:

Forms:
Form DDXXX – For each form, the plan should include the purpose the SSN serves as well as potential alternatives. Some level of detail regarding the owner of the form and any pertinent details regarding the form owners plan to eliminate the use of the SSN.

Systems:
XXX System – For each system that provides an input to the system or is responsible for generating the form, the plan should discuss the purpose served by the SSN and any potential alternatives. Some level of detail should 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 should 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:

Dated: February 23, 2010.

Patricia L. Toppings,

OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2010–4290 Filed 3–2–10; 8:45 am]

BILLING CODE 5001–06–C