INFORMATION PAPER

Date here

Department of Defense Identification Number

The social security number (SSN) has been used throughout the Department of Defense (DoD) as a means to identify and authenticate individuals and its expanded use 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 to eliminate its unnecessary use where possible.

One effort initiated to reduce the use of the SSN is to replace it with the number known as the Electronic Data Interchange-Personal Identifier (EDI-PI) that has been a unique identifier for personnel affiliated with the DoD for many years. Until recently, it was used only by DoD information systems to facilitate machine-to-machine communications and appeared in digital signatures. When the EDI-PI was selected to become the DoD identification number (DoD ID Number), the purpose of the identifier changed.

The expanded use of the DoD ID Number has led to questions regarding its status as personally identifiable information (PII). PII refers to information that can be used to distinguish or trace an individual's identity. The DoD ID Number falls into this category because it is a unique personal identifier and can be used to retrieve records about an individual.

The DoD ID Number is now intended to be known by the individual to whom it belongs, and is printed on DoD identification cards. It is to be used for individual access to systems, on forms, in digital signatures and for other uses typical of physical and technical identification processes.

The DoD ID Number shall only be used for DoD business purposes and may include transactions with entities outside DoD, so long as individuals are acting on behalf of or in support of the DoD. The DoD ID 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 ID Number are managed and administered for the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) by the Defense Manpower Data Center (DMDC) and must include at a minimum these stipulations:

The DoD ID Number cannot be used for any purpose not identified in the agreement. The recipient agency must agree not to share the DoD ID Number with any other agency or outside organization without the permission of the DoD, and that the DoD ID Number will not be used for single factor authentication, but will instead be used as one factor in a multi-factor authentication process.

241 18th Street South, Suite 101 | Arlington VA 22202

703.571.0070 | dpclo.defense.gov

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

The DoD ID Number, by itself or with an associated name, shall be considered internal government operations-related PII. Since the loss, theft or compromise of the DoD ID Number has a low risk for possible identity theft or fraud, a PII breach report will not be initiated unless the breach is associated with other PII elements, such as date of birth, birthplace or mother's maiden name, which would normally require a report to be submitted. As detailed in DoDI 1000.30, "Reduction of Social Security Number (SSN) Use Within DoD", exposure of the DoD ID Number shall not be considered a breach when exposed as a part of a DoD business function.

It is common practice today to use digital signatures, which contain an individual's DoD ID Number, on documents and emails. These documents and emails when sent outside the department may be made public in the authorized release of records, thereby exposing the DoD ID Number. Digital signatures, therefore, would not constitute a breach, even if exposed externally. If exposed through a breach, and not in association with a DoD business process, loss of the DoD ID Number alone should generally be considered a low risk breach.

References/Related Links:

DoDI 1000.30, "Reduction of Social Security Number (SSN) Use Within DoD", August 1, 2012 http://www.dtic.mil/whs/directives/corres/pdf/100030p.pdf

November 5, 2010 Memorandum entitled, "Updated Plan for the Removal of Social Security numbers (SSNs) from Department of Defense (DoD) Identification (ID) Cards"

http://dpclo.defense.gov/privacy/documents/SSN%20from%20ID%20Cards.pdf