

Reporting Requirements Incident to Breaches of Personally Identifiable Information

Major Scott E. Dunn¹

All Army Activities (ALARACT) message number 050/2009¹ sets forth stringent reporting requirements for reporting unauthorized access to personally identifiable information (PII). The ALARACT defines PII as “any information about an individual which can be used to distinguish or trace an individual’s identity such as name, social security number, date and place of birth, mother’s maiden name, and biometric records.”² A PII breach or compromise incident occurs “when it is suspected or confirmed that PII is lost, stolen, or otherwise available to individuals without a duty related official need to know.”³

Once such an incident is suspected, the following reports and notifications are required: report to the U.S. Computer Emergency Response Team (US-CERT) within one hour;⁴ concurrently, send an e-mail to PII.Reporting@us.army.mil to inform Army leadership;⁵ and report to the Army FOIA/Privacy Office within twenty-four hours.⁶ These reports are in addition to, not in lieu of, any command notification requirements that may also apply (such as Serious Incident Reports, etc.).⁷ Notification of affected individuals may also be required, depending on the severity of the breach.⁸ The ALARACT contains more information concerning the required formats of the reports.

Department of Defense Initiative to Reduce the Use of Social Security Numbers (SSNs)

Major Scott E. Dunn

Military agencies routinely use social security numbers (SSNs) for a number of purposes, often without good reason.⁹ Common, and sometimes unnecessary, use of SSNs increases the risk to servicemembers of identity theft.¹⁰ The Department of Defense (DoD) is aware of the problem and has sought to address this in an ongoing initiative to reduce its use of SSNs.¹¹ The primary components of the initiative are twofold: first, a review of all official forms within DoD to ensure that SSNs are only required when there is a good reason for it;¹² and second, the eventual adoption of alternative forms of identification for most routine business practices within DoD.¹³ Most notably, this initiative will eventually result in the elimination of visible SSNs from DoD identification cards¹⁴ and the use of DoD identification numbers and DoD benefits numbers instead.¹⁵

¹ Judge Advocate, U.S. Army. Presently assigned as Associate Professor, Administrative and Civil Law Department, The Judge Advocate General's Legal Center and School, Charlottesville, Virginia.

² Message, 262121Z Feb 09, U.S. Dep't of Army, subject: ALARACT 050/2009, Personally Identifiable Information (PII) Incident Reporting and Notification Procedures para. 2.

³ *Id.* para. 3.

⁴ *Id.* para. 4.1.

⁵ *Id.*

⁶ *Id.* para. 4.2.

⁷ *Id.* para. 4.3.

⁸ *Id.* para. 4.5.

⁹ See, e.g., Gregory Conti et al., *The Military's Cultural Disregard for Personal Information*, SMALL WARS J., Dec 6, 2010, <http://smallwarsjournal.com/blog/journal/docs-temp/615-conti.pdf>.

¹⁰ *Id.* at 1.

¹¹ Memorandum from Undersec'y of Def., Personnel & Readiness, for Sec'ys of the Military Dep'ts et al., subject: Directive-Type Memorandum (DTM) 2007-015-USD(P&R)—“DoD Social Security Number (SSN) Reduction Plan” (28 Mar. 2008) (incorporating C1, 29 Nov. 2010).

¹² *Id.* attachment 2.

¹³ *Id.* attachment 2, para. 4.

¹⁴ Memorandum from Undersec'y of Def., Personnel & Readiness, for Sec'ys of the Military Dep'ts et al., subject: Updated Plan for the Removal of Social Security Numbers (SSNs) from Department of Defense (DoD) Identification (ID) Cards (5 Nov. 2010).

¹⁵ *Id.* at 3.