(5) The format of the lost, stolen or improperly accessed data, e.g., in a standard electronic format, such as ASCII, or in paper;

(6) Evidence indicating that the lost, stolen or improperly accessed data may have been the target of unlawful acquisition; and

(7) Evidence that the same or similar data had been acquired from other sources improperly and used for identity theft.

(c) VA will provide notice and/or other credit protection services under this section as provided in §§ 75.117 and 75.118.

(Authority: 38 U.S.C. 501, 5724, 5727)

§ 75.115 Risk analysis.

If a data breach involving sensitive personal information that is processed or maintained by VA occurs and the Secretary has not determined under § 75.114 that an accelerated response is appropriate, the Secretary shall ensure that, as soon as possible after the data breach, a non-VA entity with relevant expertise in data breach assessment and risk analysis or VA's Office of Inspector General conducts an independent risk analysis of the data breach. The preparation of the risk analysis may include data mining if necessary for the development of relevant information. The risk analysis shall include a finding with supporting rationale concerning whether the circumstances create a reasonable risk that sensitive personal information potentially may be misused. If the risk analysis concludes that the data breach presents a reasonable risk for the potential misuse of sensitive personal information, the risk analysis must also contain operational recommendations for responding to the data breach. Each risk analysis, regardless of findings and operational recommendations, shall also address all relevant information concerning the data breach, including the following:

(a) Nature of the event (loss, theft, unauthorized access).

(b) Description of the event, including:

(1) Date of occurrence;

(2) Data elements involved, including any personally identifiable information, such as full name, social security number, date of birth, home address, account number, disability code;

(3) Number of individuals affected or potentially affected;

(4) Individuals or groups affected or potentially affected;

(5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

(6) Time the data has been out of VA control;

(7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons); and

(8) Known misuses of data containing sensitive personal information, if any.

(c) Assessment of the potential harm to the affected individuals.

(d) Data breach analysis, as appropriate.

(Authority: 38 U.S.C. 501, 5724, 5727)

§ 75.116 Secretary determination.

(a) Upon receipt of a risk analysis prepared under this subpart, the Secretary will consider the findings and other information contained in the risk analysis to determine whether the data breach caused a reasonable risk for the potential misuse of sensitive personal information. If the Secretary finds that such a reasonable risk does not exist, the Secretary will take no further action under this subpart. However, if the Secretary finds that such a reasonable risk exists, the Secretary will take responsive action as specified in this subpart based on the potential harms to individuals subject to a data breach.

(b) In determining whether the data breach resulted in a reasonable risk for the potential misuse of the compromised sensitive personal information, the Secretary shall consider all factors that the Secretary, in his or her discretion, considers relevant to the decision, including:

(1) The likelihood that the sensitive personal information will be or has been made accessible to and usable by unauthorized persons;

(2) Known misuses, if any, of the same or similar sensitive personal information;

(3) Any assessment of the potential harm to the affected individuals provided in the risk analysis;

(4) Whether the credit protection services that VA may offer under 38 U.S.C. 5724 may assist record subjects in avoiding or mitigating the results of identity theft based on the VA sensitive personal information that had been compromised;

(5) Whether private entities are required under Federal law to offer credit protection services to individuals if the same or similar data of the private entities had been similarly compromised; and

(6) The recommendations, if any, concerning the offer of, or benefits to be derived from, credit protection services in this case that are in the risk analysis report.

(Authority: 38 U.S.C. 501, 5724, 5727)

§ 75.117 Notification.

(a) With respect to individuals found under this subpart by the Secretary to be subject to a reasonable risk for the potential misuse of any sensitive personal information, the Secretary will promptly provide written notification by first-class mail to the individual (or the next of kin if the individual is deceased) at the last known address of the individual. The notification may be sent in one or more mailings as information is available and will include the following:

(1) A brief description of what happened, including the date[s] of the data breach and of its discovery if known;

(2) To the extent possible, a description of the types of personal information that were involved in the data breach (e.g., full name, Social Security number, date of birth, home address, account number, disability code);

(3) A brief description of what the agency is doing to investigate the breach, to mitigate losses, and to protect against any further breach of the data;

(4) Contact procedures for those wishing to ask questions or learn additional information, which will include a toll-free telephone number, an e-mail address, Web site, and/or postal address;

(5) Steps individuals should take to protect themselves from the risk of identity theft, including steps to obtain fraud alerts (alerts of any key changes to such reports and on demand personal access to credit reports and scores), if appropriate, and instruction for obtaining other credit protection services offered under this subpart; and

(6) A statement whether the information was encrypted or protected by other means, when determined such information would be beneficial and would not compromise the security of the system.

(b) In those instances where there is insufficient, or out-of-date contact information that precludes direct written notification to an individual subject to a data breach, a substitute form of notice may be provided, such as a conspicuous posting on the home page of VA's Web site and notification in major print and broadcast media, including major media in geographic areas where the affected individuals likely reside. Such a notice in media will include a toll-free phone number where an individual can learn whether or not his or her personal information is possibly included in the data breach.

(c) In those cases deemed by the Secretary to require urgency because of possible imminent misuse of sensitive personal information, the Secretary, in addition to notification under paragraph (a) of this section, may provide information to individuals by telephone or other means, as appropriate.

(d) Notwithstanding other provisions in this section, notifications may be delayed upon lawful requests, from other Federal agencies, for the delay of notifications in order to protect data or computer resources from further compromise or to prevent interference with the conduct of an investigation or efforts to recover the data. A lawful request is one made in writing by the entity or VA component responsible for the investigation or data recovery efforts that may be adversely affected by providing notification. Any lawful request for delay in notification must state an estimated date after which the requesting entity believes that notification will not adversely affect the conduct of the investigation or efforts to recover the data. However, any delay should not exacerbate risk or