significant economic impact on a substantial number of small entities as they are defined in the Regulatory Flexibility Act. This amendment will not directly affect any small entities. Therefore, this amendment is also exempt pursuant to 5 U.S.C. 605(b) from the initial and final regulatory flexibility analysis requirements of sections 603–604.

Catalog of Federal Domestic Assistance

There are no Catalog of Federal Domestic Assistance program numbers for this rule.

List of Subjects in 38 CFR Part 2

Authority delegations (Government agencies).

Approved: June 15, 2007.

Gordon H. Mansfield,

Deputy Secretary of Veterans Affairs.

■ For the reasons set forth in the preamble, 38 CFR part 2 is amended as follows:

PART 2—DELEGATIONS OF AUTHORITY

■ 1. The authority citation for part 2 continues to read as follows:

Authority: 5 U.S.C. 302, 552a; 38 U.S.C. 501, 512, 515, 1729, 1729A, 5711; 44 U.S.C. 3702, and as noted in specific sections.

■ 2. Amend § 2.6 by:

■ a. In paragraph (l)(1), removing ''Secretary'' and adding, in its place, ''Secretary, the Deputy Secretary,''.

■ b. Revising paragraph (l)(3).

The revision reads as follows:

§ 2.6 Secretary's delegations of authority to certain officials (38 U.S.C. 512).

* * * * *

(l) * * *

(3) To serve as the Deputy Regulatory Policy Officer, to perform staff functions under the Regulatory Policy Officer, and to perform other delegated functions in accordance with Executive Order 12866.

* * * * *

[FR Doc. E7–12058 Filed 6–21–07; 8:45 am]

BILLING CODE 8320–01–P

DEPARTMENT OF VETERANS AFFAIRS

38 CFR Part 75

RIN 2900–AM63

Data Breaches

AGENCY: Department of Veterans Affairs.

ACTION: Interim final rule.

SUMMARY: This document establishes regulations to address data breaches regarding sensitive personal information that is processed or maintained by the Department of Veterans Affairs (VA). The regulations implement certain provisions of Title IX of the Veterans Benefits, Health Care, and Information Technology Act of 2006, which require promulgation of these regulations as an interim final rule.

DATES: *Effective Date:* This interim final rule is effective on June 22, 2007. Comments must be received on or before August 21, 2007.

ADDRESSES: Written comments may be submitted through *www.Regulations.gov;* by mail or hand-delivery to the Director, Regulations Management (00REG), Department of Veterans Affairs, 810 Vermont Ave., NW., Room 1068, Washington, DC 20420; or by fax to (202) 273–9026. Comments should indicate that they are submitted in response to ''RIN 2900–AM63–Data Breaches.'' Copies of comments received will be available for public inspection in the Office of Regulation Policy and Management, Room 1063B, between the hours of 8 a.m. and 4:30 p.m. Monday through Friday (except holidays). Please call (202) 273–9515 for an appointment. (This is not a toll-free number.) In addition, during the comment period, comments may be viewed online through the Federal Docket Management System (FDMS) at *www.Regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Terry Simmons, Information Technology Specialist, Office of Information Protection and Risk Management (005T), (202) 461–9217, Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420. (This is not a toll-free number.)

SUPPLEMENTARY INFORMATION: This document establishes regulations captioned ''Data Breaches'' (referred to below as the regulations). The regulations implement 38 U.S.C. 5724 and 5727, which were enacted as part of Title IX of Public Law 109–461, the Veterans Benefits, Health Care, and Information Technology Act of 2006. VA will promulgate regulations to implement 38 U.S.C. 5722 and 5723, which were also enacted as part of Title IX of Public Law 109–461, in a separate rulemaking.

The regulations, which follow the statutory framework set out in section 5724, prescribe a mechanism for taking actions in response to a data breach of sensitive personal information. The finding of a data breach of sensitive personal information normally triggers a risk analysis. A risk analysis provides the basis for a determination as to whether individuals subject to a data breach will be given notice of the data breach and any other credit protections services authorized by VA. Under section 5724, VA must provide at least one credit protection service upon a finding that a reasonable risk exists for the potential misuse of sensitive personal information involved in a data breach. Consistent with this authority, the regulations require compliance with notification provisions when such finding occurs. The regulations also require that other credit protection services be provided, if warranted, based on the consideration of specified factors.

However, section 5724 does not bar the Secretary from acting promptly to address a data breach without first conducting a risk analysis where the situation dictates. If the information available to the agency indicates that there is an immediate, substantial risk of identity theft of the individuals whose data was the subject of the data breach, the Secretary may notify the record subjects of the breach promptly so that they may take steps to protect themselves, and also may offer them other credit protection services without conducting a risk analysis. Additionally, the Secretary may offer credit protection services to individuals without first performing a risk analysis where a previous risk analysis performed by VA or another Federal agency involving the same or similar data determined that it was appropriate to offer the subject individuals credit protection services, including providing notice of the data breach. Finally, the Secretary may provide an initial notice of the data breach prior to completion of the risk analysis where private entities would be required to provide notice under Federal law if they experienced a data breach involving the same or similar information. In this last situation, the Secretary may provide notice of the breach and subsequently advise individuals whether the agency will offer additional credit protection services upon completion, and consideration of the results, of any risk analysis.

Contents of this regulation, including notification of data breaches which may result in harms other than identity theft, should be interpreted to be consistent with OMB Memorandum M–07–16, ''Safeguarding Against and Responding to Breaches of Personally Identifiable Information.'' The regulations are set forth as Subpart B in new 38 CFR part 75. Subpart A is reserved.

Section 75.111 Purpose and Scope

The purpose and scope section explains that the regulations implement

38 U.S.C. 5724 and 5727 and that the regulations concern actions to address data breaches of sensitive personal information that is processed or maintained by VA. Thus, the regulations apply to sensitive personal information stored on VA computer systems, as well as to VA sensitive information stored on non-VA computer systems for VA, such as by a contractor. VA employees and contractors legally may perform activities for VA and for others. Those duties often require the collection, use and maintenance of sensitive personal information for both VA and for the other entity on a common electronic storage medium, such as a hard drive on a server. In these instances, the VA data are to be partitioned or segregated, such as being stored on separate virtual servers. Various factors may be different for the VA and non-VA data. For example, the data may be different, may have different levels of security or be in different formats. Finally, the legal protections required for the data, as well as the legal responsibilities for the data may be different. Consequently, the regulations apply only to VA data in this situation. The owners of the other, non-VA data residing on a non-VA storage medium that is lost, stolen or improperly accessed are responsible for identifying and complying with the legal requirements that those owners consider applicable to their data.

Based on our interpretation of the statutory requirements, we have also added a statement indicating that the regulations do not supersede the requirements imposed by other laws, such as the Privacy Act of 1974, the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, the Fair Credit Reporting Act, and implementing regulations of such Acts.

Section 75.112 Definitions and Terms

So that the full terms would not have to be written out each time they are used in the regulations, ''VA'' means the Department of Veterans Affairs, and ''Secretary'' means the Secretary of Veterans Affairs or designee.

The following definitions are exactly the same or the same in substance as the corresponding definitions in the authorizing legislation at 38 U.S.C. 5727: ''confidentiality,'' ''data breach,'' ''data breach analysis,'' ''fraud resolution services,'' ''identity theft,'' ''identity theft insurance,'' ''information system,'' ''integrity,'' and ''sensitive personal information.''

The term ''individual'' is used in the definition of the phrase ''sensitive personal information,'' but is itself undefined in the statute. We have defined ''individual'' to mean a single human being who is a citizen of the United States, an alien admitted to permanent residence in the United States, a present or former member of the Armed Forces, or any dependent of a present or former member of the Armed Forces. The first two parts of this definition come from the Privacy Act of 1974, 5 U.S.C. 552a(a)(2), and the last two parts come from 38 U.S.C. 5701(a), which specifically provides confidentiality for the names and home addresses of present or former members of the Armed Forces and their dependents. It was apparent during the Congressional hearings after the May 2006 data breach involving the employee hard drive stolen from his home that the Members' focus was on the possible impact of a data breach on those individuals on whom VA normally maintains individually-identified information. The definition of ''individual'' to include the human beings on whom VA maintains data is consistent with this Congressional concern.

The phrase ''unauthorized access * * * incidental to the scope of employment'' is included in the statutory definition of data breach. We have defined this phrase to have the meaning that we believe was intended by the statutory authority.

We defined ''person'' consistent with its common use when intended to include individuals and entities and consistent with its use in other VA regulations (see 38 CFR 1.460).

We defined ''processed or maintained by VA'' to include all actions by VA regarding sensitive personal information for which VA has responsibility under the statutory authority of 38 U.S.C. 5724 and 5727.

Section 75.113 Data Breach

Consistent with the definition of ''data breach'' in the definition section, the regulations provide that a data breach occurs if there is a loss, theft, or other unauthorized access, other than an unauthorized access incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. To clarify the scope of the regulations, we explain that the term ''unauthorized access'' used in the definition of ''data breach'' includes access to an electronic information system and includes, but is not limited to, viewing, obtaining, or using data containing sensitive personal information in any form or in any VA information system. The phrase ''unauthorized access incidental to the scope of employment'' includes instances when employees of contractors and other entities need access to VA sensitive information in order to perform a contract or agreement with VA but incidentally obtain access to other VA sensitive information. In accordance with this explanation, an unauthorized access, other than an unauthorized access incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, which results in the potential compromise of the confidentiality or integrity of the data, constitutes a data breach. Also, in § 75.113, we note that VA interprets data breach to include circumstances in which a user misuses sensitive personal information to which he or she has authorized access.

To help interested individuals understand our view of what is not included in the definition of data breach, and, consequently, what is not subject to the provisions of the regulations, we have added an example in § 75.113(a) to illustrate when an occurrence constitutes an unauthorized access incidental to the scope of employment.

The following is a specific example of unauthorized access that is incidental to employment and therefore does not constitute a data breach. Contractor A has a contract to perform service 1 for VA. The contractor needs access to sensitive personal information to perform the contract. Contractor B also has a contract to perform service 2 for which contractor B needs access to sensitive personal information in order to perform the contract. The sensitive data in each contract is substantially the same, e.g., VA beneficiary demographic information for different groups of beneficiaries. Both contractors have complied with all applicable security and privacy requirements to access and use the data to perform each contract. A VA employee inadvertently provides contractor B with a CD with the encrypted data that contractor A needs to perform its contract. At the same time, the employee inadvertently also provides in a separate communication the password to decrypt the file. Contractor B opens the encrypted file, realizes that the sensitive personal information in the file is not the data that it needs to perform contract 2. Contractor B immediately closes and properly re-encrypts the data file and returns the CD to the appropriate VA official. Contractor B did not retain a copy of the data on the CD. Contractor B's access to the data file needed by Contractor A is an inadvertent unauthorized viewing of sensitive

personal information by a person acting on behalf of VA and therefore is not a data breach.

We also have added examples in § 75.113(b) to illustrate when an occurrence would not be one ''that results in the potential compromise of the confidentiality or integrity of the data.'' The addition of the clause ''that results in the potential compromise of the confidentiality or integrity of the data'' could not have been intended to mean zero percent possibility of creating a compromise of the confidentiality or integrity of the data, since such zero percent possibility would have applied if the clause had not been added. In our view, in order to trigger the need for a risk analysis, the added clause is appropriately interpreted to mean that a loss, theft, or other unauthorized access to data containing sensitive personal information that has even a minimal possibility of compromising the confidentiality or integrity of data constitutes a data breach and the examples reflect this conclusion.

The following is another concrete example of an event that does not constitute a data breach. An employee is transporting a CD containing an encrypted flat file containing sensitive personal information. The file is encrypted using a software program that has been certified by the National Institute of Standards and Technology (NIST) as complying with the most recent security standards and certification of cryptographic modules. The vehicle in which the employee is riding crashes through a bridge railing and falls into a river. The car and the CD are recovered, and it is determined that the CD is destroyed. The likelihood that the CD will be recovered is minimal, and if recovered, the encryption would not permit access to the data. Therefore, there is no possibility of compromising the confidentiality or integrity of the data, and accordingly, this is not a data breach.

Section 75.114 Accelerated Response

If the information available to the agency when VA learns of the data breach indicates that there is an immediate, substantial risk of identity theft for individuals as a result of the data breach, prior to completing a risk analysis, the Secretary may promptly notify the record subjects of the breach, and/or offer them other credit protection services as the Secretary determines in the exercise of his or her discretion what would be likely to assist the record subjects in preventing, or mitigating the results of, identity theft based on the compromised VA sensitive personal information. Additionally, Secretary may provide initial notice of the data breach without, or prior to completion of, a risk analysis where private entities would be required to provide notice under Federal law if they experienced a data breach involving the same or similar information. In such cases, the Secretary may provide notice of the breach and subsequently advise individuals whether the agency will offer additional credit protection services upon completion and consideration of the results of the risk analysis. The agency will provide the notice and/or other credit protection services under this section in accordance with §§ 75.117 and 75.118 of these regulations.

Section 75.115 Risk Analysis

Under 38 U.S.C. 5724, VA must ensure that, as soon as possible after a data breach, a non-VA entity or the VA Office of Inspector General conducts an independent risk analysis of the data breach (which under 38 U.S.C. 5724 may include data mining as necessary to obtain relevant information) to determine the level of risk for potential misuse of sensitive personal information. To provide information that the Secretary will use in making determinations required under the regulations, this section requires that the risk analysis address identified factors relating to risks and potential harms.

Section 75.116 Secretary Determination

Under 38 U.S.C. 5724, VA must consider the findings of each risk analysis and determine, based on criteria in the regulation, whether a reasonable risk exists for the potential misuse of sensitive personal information involved in a data breach. Consistent with the statutory intent, this section indicates that VA will take no further action under the regulations upon a finding that such a reasonable risk does not exist. Also, consistent with the statutory intent, this section indicates that VA will take further action as provided under the regulations (discussed below) upon a finding that a data breach of sensitive personal information poses a reasonable risk of potential misuse.

Section 75.117 Notification

To implement 38 U.S.C. 5724, we are establishing procedures for notifying individuals whose sensitive personal information are subject to a reasonable risk for potential misuse from a data breach. Under this statutory provision, we have authority to provide notification once there is a finding that a reasonable risk exists for the potential misuse of any sensitive personal information involved in the data breach. The regulations reflect our view that the notification procedures should be utilized whenever this threshold determination is made by the Secretary.

Paragraph (a) includes the information that we believe should be provided to affected individuals to ensure that they understand what has happened and what they can expect from VA with regard to other credit protection services. Under paragraph (a), affected individuals will receive letters sent via first-class mail explaining the circumstances of the data breach and possible responses for such individuals. We believe that this is an effective means of providing information. However, paragraph (b) contains alternative means of providing information if we are unable to contact an affected individual by mail. Further, paragraph (c) clarifies that VA will also provide notification using a quicker method, such as notification by telephone, when there is a possible imminent misuse of sensitive personal information due to a data breach. However, we have also included information in paragraph (d) explaining that in determining when to provide notification, we will consider lawful requests, from other Federal agencies, for the delay of notifications in order to prevent interference with the conduct of an investigation or efforts to recover the data.

Section 75.118 Other Credit Protection Services

Under 38 U.S.C. 5724, VA may provide other credit protection services to individuals found to be subject to a reasonable risk for the potential misuse of any sensitive personal information because of a data breach. VA is specifically authorized to provide credit monitoring, data breach analysis, fraud resolution services, and identity theft insurance. Accordingly, the Secretary may offer one or more of the following if warranted based on considerations specified below:

- One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports (this is a standard credit monitoring policy);
- Data breach analysis;
- Fraud resolutions services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution; and/or
- One year of identity theft insurance with $20,000.00 coverage at $0

deductible (this is a standard identity theft insurance policy).

The determination by the Secretary regarding whether any or all of these credit protection services will be offered to individuals subject to a data breach will depend on the particular facts in a case. Accordingly, we have established the following considerations for helping to determine what credit protection services will be offered to individuals subject to a data breach:

- The data elements involved;
- The number of individuals affected or potentially affected;
- The likelihood that sensitive personal information will be or has been compromised (made accessible to and usable by unauthorized persons);
- The risk of harm to the affected individuals; and
- The ability to prevent or mitigate the risk of harm by offering credit protection services.

Pursuant to authority in 38 U.S.C. 5724, the regulations also provide that VA will obtain data mining and data breach analyses services, as appropriate, to obtain information relevant for making determinations under this subpart.

Section 75.119 Finality of Secretary Determination

Under 38 U.S.C. 5724, the Secretary is required to make various determinations concerning a particular data breach incident. Any determination made by the Secretary under this subpart will be considered a final agency decision.

Solicitation of Comments

VA solicits comments on the following matters. VA will consider comments on all provisions of this Interim Final Rule received during the 60-day public comment period.

Section 75.115 Risk Analysis

VA solicits comments on use of data mining as necessary for the development of relevant information to assist in preparation of risk analysis following a data breach. In particular, we seek comments on the purposes for which data mining would be appropriate and acceptable uses of the information resulting from data mining.

Section 75.117 Notification

We are considering not providing written notification if the Secretary determines that the data breach incident has been widely disseminated through the media. Specifically, we are soliciting comment on the following possible draft provision:

(e) Notwithstanding other provisions of this section, the Secretary may forgo notification by first-class mail upon a determination that the information in paragraphs (a)(1) through (a)(5) of this section has been widely disseminated through the media, a mailing would virtually duplicate information that has already been provided to individuals subject to a data breach, and the agency can determine with reasonable certainty all of the affected individuals have received actual notice of (1) the data breach and (2) their inclusion in the affected class of individuals. In determining whether media dissemination has already provided adequate notice to affected individuals, the Secretary will also consider media coverage at the national level, and, where the data breach is limited to individuals within a particular, defined geographic area or areas, the media coverage in that area. The Secretary will further consider the extent of the accuracy of media coverage, frequency of repetition of such media coverage (number of articles or frequency of publications or broadcasts), and the variety of media outlets carrying such media coverage.

Potential Procedures for Appeals or Reconsiderations of Decisions Made Under Subpart B

Public Law 109–461 was silent regarding appeals or reconsiderations of decisions made under Section 902 Department of Veterans Affairs Information Security Programs and Requirements. VA solicits comments on potential procedures for appeals and reconsiderations.

Administrative Procedure Act

This rule is exempt from the prior notice and comment and delayed effective date provisions of 5 U.S.C. 553 for good cause because they are unnecessary based on the statutory mandate in 38 U.S.C. 5724 to publish this document as an interim final rule. 5 U.S.C. 553(b)(B), (d)(3).

Unfunded Mandates

The Unfunded Mandates Reform Act of 1995 requires, at 2 U.S.C. 1532, that agencies prepare an assessment of anticipated costs and benefits before issuing any rule that may result in expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more (adjusted annually for inflation) in any given year. This rule would have no such effect on State, local, and tribal governments or the private sector.

Paperwork Reduction Act

This document contains no provisions constituting a collection of information under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501–3521).

Executive Order 12866

Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; distributive impacts; and equity). The Executive Order classifies a ''significant regulatory action,'' requiring review by the Office of Management and Budget (OMB) unless OMB waives such review, as any regulatory action that is likely to result in a rule that may: (1) Have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, or tribal 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 the Executive Order.

The economic, interagency, budgetary, legal, and policy implications of this interim final rule have been examined and it has been determined to be a significant regulatory action under the Executive Order because it is likely to result in a rule that may raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in the Executive Order.

Regulatory Flexibility Act

The provisions of the Regulatory Flexibility Act (5 U.S.C. 601–612) do not apply to this interim final rule because the provisions of 38 U.S.C. 5724 require that this document be promulgated as an interim final rule, and, consequently, a notice of proposed rulemaking was not required for the rule. 5 U.S.C. 603–604.

Catalog of Federal Domestic Assistance Numbers

There are no Catalog of Federal Domestic Assistance numbers and titles for this rule.

List of Subjects in 38 CFR Part 75

Administrative practice and procedure, Credit monitoring, Data breach, Data breach analysis, Data mining, Fraud alerts, Identity theft insurance, Information, Notification, Risk analysis, Security measures.

Approved: June 13, 2007.

Gordon H. Mansfield,

Deputy Secretary of Veterans Affairs.

■ For reasons set forth in the preamble, VA is amending 38 CFR chapter I by adding part 75 to read as follows:

PART 75—INFORMATION SECURITY MATTERS

Subpart A—[Reserved]

Subpart B—Data Breaches

Sec.

75.111 Purpose and scope.
75.112 Definitions and terms.
75.113 Data breach.
75.114 Accelerated response.
75.115 Risk analysis.
75.116 Secretary determination.
75.117 Notification.
75.118 Other credit protection services.
75.119 Finality of Secretary determination.

Authority: 38 U.S.C. 501, 5724, 5727, 7906.

Subpart A—[Reserved]

Subpart B—Data Breaches

§ 75.111 Purpose and scope.

This subpart implements provisions of 38 U.S.C. 5724 and 5727, which are set forth in Title IX of the Veterans Benefits, Health Care, and Information Technology Act of 2006. It only concerns actions to address a data breach regarding sensitive personal information that is processed or maintained by VA. This subpart does not supersede the requirements imposed by other laws, such as the Privacy Act of 1974, the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, the Fair Credit Reporting Act, and implementing regulations of such Acts.

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

§ 75.112 Definitions and terms.

For purposes of this subpart:

Confidentiality means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

Data breach means the loss or theft of, or other unauthorized access to, other than an unauthorized access incidental to the scope of employment, data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data.

Data breach analysis means the process used to determine if a data breach has resulted in the misuse of sensitive personal information.

Fraud resolution services means services to assist an individual in the process of recovering and rehabilitating the credit of the individual after the individual experiences identity theft.

Identity theft has the meaning given such term under section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a).

Identity theft insurance means any insurance policy that pays benefits for costs, including travel costs, notary fees, and postage costs, lost wages, and legal fees and expenses associated with efforts to correct and ameliorate the effects and results of identity theft of the insured individual.

Individual means a single human being who is a citizen of the United States, an alien admitted to permanent residence in the United States, a present or former member of the Armed Forces, or any dependent of a present or former member of the Armed Forces.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual.

Integrity means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Logical data access means the ability of a person to translate the data for misuse. This can lead to inappropriate access to lost, stolen or improperly obtained data.

Person means an individual; partnership; corporation; Federal, State, or local government agency; or any other legal entity.

Processed or maintained by VA means created, stored, transmitted, or manipulated by VA personnel or by a person acting on behalf of VA, including a contractor or other organization or any level of subcontractor or other suborganization.

Secretary means the Secretary of Veterans Affairs or designee.

Sensitive personal information, with respect to an individual, means any information about the individual maintained by an agency, including the following:

(1) Education, financial transactions, medical history, and criminal or employment history.

(2) Information that can be used to distinguish or trace the individual's identity, including name, Social Security number, date and place of birth, mother's maiden name, or biometric records.

Unauthorized access incidental to the scope of employment means access, in accordance with VA data security and confidentiality policies and practices, that is a by-product or result of a permitted use of the data, that is inadvertent and cannot reasonably be prevented, and that is limited in nature.

VA means the Department of Veterans Affairs.

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

§ 75.113 Data breach.

Consistent with the definition of data breach in § 75.112 of this subpart, a data breach occurs under this subpart if there is a loss or theft of, or other unauthorized access to, other than an unauthorized access incidental to the scope of employment, data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. The term ''unauthorized access'' used in the definition of ''data breach'' includes access to an electronic information system and includes, but is not limited to, viewing, obtaining, or using data containing sensitive personal information in any form or in any VA information system. The phrase ''unauthorized access incidental to the scope of employment'' includes instances when employees of contractors and other entities need access to VA sensitive information in order to perform a contract or agreement with VA but incidentally obtain access to other VA sensitive information. Accordingly, an unauthorized access, other than an unauthorized access incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data, constitutes a data breach. In addition to these circumstances, VA also interprets data breach to include circumstances in which a user misuses sensitive personal information to which he or she has authorized access. The following circumstances do not constitute a data breach and, consequently, are not subject to the provisions of this subpart:

(a) An unauthorized access to data containing sensitive personal information that was determined by the Secretary to be incidental to the scope of employment, such as an inadvertent unauthorized viewing of sensitive personal information by a VA employee or a person acting on behalf of VA.

(b) A loss, theft, or other unauthorized access to data containing sensitive personal information that the Secretary determined to have no possibility of compromising the confidentiality or integrity of the data, such as the inability of compromising the

confidentiality or integrity of the data because of encryption or the inadvertent disclosure to another entity that is required to provide the same or a similar level of protection for the data under statutory or regulatory authority.

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

§ 75.114 Accelerated response.

(a) The Secretary, in the exercise of his or her discretion, may provide notice to records subjects of a data breach and/or offer them other credit protection services prior to the completion of a risk analysis if:

(1) The Secretary determines, based on the information available to the agency when it learns of the data breach, that there is an immediate, substantial risk of identity theft of the individuals whose data was the subject of the data breach, and providing timely notice may enable the record subjects to promptly take steps to protect themselves, and/or the offer of other credit protection services will assist in timely mitigation of possible harm to individuals from the data breach; or

(2) Private entities would be required to provide notice under Federal law if they experienced a data breach involving the same or similar information.

(3) In situations described in paragraphs (a)(1) or (a)(2) of this section, the Secretary may provide notice of the breach prior to completion of a risk analysis, and subsequently advise individuals whether the agency will offer additional credit protection services upon completion, and consideration of the results, of the risk analysis, if the Secretary directs that one be completed.

(b) In determining whether to promptly notify individuals and/or offer them other credit protection services under paragraph (a)(1) of this section, the Secretary shall make the decision based upon the totality of the circumstances and information available to the Secretary at the time of the decision, including whether providing notice and offering other credit protection services would be likely to assist record subjects in preventing, or mitigating the results of, identity theft based on the compromised VA sensitive personal information. The Secretary's exercise of this discretion will be based on good cause, including consideration of the following factors:

(1) The nature and content of the lost, stolen or improperly accessed data, *e.g.*, the data elements involved, such as name, social security number, date of birth;

(2) The ability of an unauthorized party to use the lost, stolen or improperly accessed data, either by itself or with data or applications generally available, to commit identity theft or otherwise misuse the data to the disadvantage of the record subjects, if able to access and use the data;

(3) 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;

(4) Ease of physical access to the lost, stolen or improperly accessed data, *e.g.*, the degree to which the data is readily available to unauthorized access, such as being in a dumpster readily accessible by members of the general public;

(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 harm to any affected individual(s). Decisions to delay notification should be made by the Secretary.

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

§ 75.118 Other credit protection services.

(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 under this subpart, the Secretary may offer one or more of the following as warranted based on considerations specified in paragraph (b) of this section:

(1) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;

(2) Data breach analysis;

(3) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution; and/or

(4) One year of identity theft insurance with $20,000.00 coverage at $0 deductible.

(b) Consistent with the requirements of the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*) as interpreted and applied by the Federal Trade Commission, the notice to the individual offering other credit protection services will explain how the individual may obtain the services, including the information required to be submitted by the individual to obtain the services, and the time period within which the individual must act to take advantage of the credit protection services offered.

(c) In determining whether any or all of the credit protection services specified in paragraph (a) of this section will be offered to individuals subject to a data breach, the Secretary will consider the following:

(1) The data elements involved;

(2) The number of individuals affected or potentially affected;

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

(4) The risk of potential harm to the affected individuals; and

(5) The ability to mitigate the risk of harm.

(c) The Secretary will take action to obtain data mining and data breach analyses services, as appropriate, to obtain information relevant for making determinations under this subpart.

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

§ 75.119 Finality of Secretary determination.

A determination made by the Secretary under this subpart will be a final agency decision.

[FR Doc. 07–3085 Filed 6–20–07: 9:50 am]

BILLING CODE 8320–01–P

ENVIRONMENTAL PROTECTION AGENCY

40 CFR Part 180

[EPA–HQ–OPP–2006–0523; FRL–8133–6]

Thiamethoxam; Pesticide Tolerance

AGENCY: Environmental Protection Agency (EPA).

ACTION: Final rule.

SUMMARY: This regulation establishes tolerances for combined residues of thiamethoxam and its metabolite (CGA–322704) in or on artichoke, globe; caneberry subgroup 13-A, hop, dried cones; grape; grape, raisin; brassica,