State of Illinois
Department of Central Management Services

ACTION PLAN FOR NOTIFICATION OF A SECURITY BREACH

Effective August 31, 2007

Publication Name(s): **Version #(1):**

ILLINOIS DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
ACTION PLAN FOR NOTIFICATION
OF A SECURITY BREACH

PROCESS, PROCEDURE, & STANDARD PUBLICATIONS

APPROVER	Print Name	Signature	Date
DIVISION HEAD	Rafael Diaz		8/31/07
APPROVER	Print Name	Signature	Date
LEGAL COUNSEL	Dominic Saebeler		8/31/07

Instructions:

1. **Complete signature process**
2. **Digitally scan entire publication (including Publication Approval Form)**
3. **E-mail pdf version of entire publication to:** CMS.BCCS.ServiceEngineeringTeam@Illinois.gov

A. Purpose
To support the CMS policy regarding Data Breach Notification and provide direction for necessary actions to be taken.

B. Owner
BCCS Chief Information Security Officer.

C. Audience
Agencies, Boards and Commissions under the control of the Governor.

D. Required Items
N/A

E. Pre Requisites
N/A

F. Post Activities
N/A

G. Specific Instructions/Requirements

The Department of Central Management Services ("CMS") independently and in conjunction with multiple State Agencies is responsible for handling a great deal of information; included in that information is private or personal information. CMS actively takes reasonable precautions to protect such information in electronic or hard copy format. CMS manages its own information as well as that of multiple State Agencies that also collect and manage such information.

The goal of this action plan is to support the overall CMS policy regarding breach notification and information security and provide a clear direction to achieve that goal.

Public Act 94-35 created the Personal Information Protection Act (815 ILCS 530/) that became effective January 1, 2006. The Act was amended by PA 94-947 on June 27, 2006. The Act defines personal information as:

Personal information means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name of the data elements are not encrypted or redacted:

1. Social Security number;
2. Driver's license number or State Identification card number;
3. Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;

CMS has and will continue to take precautions, and advise Agencies that it supports, to protect personal information; however, if CMS or a State Agency identifies a specific data breach or "breach of the security of the system data" as defined in the Statute to be the "unauthorized

acquisition of computerized data that comprises the security, confidentiality, or integrity of the personal information maintained by the data collector.", CMS or such Agency should comply with the Personal Information Protection Act, which includes notifying affected individuals of the security breach by invoking the following action plan.

CMS Action Plan

Generally, early notification to individuals whose personal information has been comprised allows them to take steps to mitigate the misuse of their information. In deciding if notification is warranted, CMS and/or the Agency should consider the nature of the compromise, the type of information taken, the likelihood of misuse, and the potential damage arising from misuse. For example, if names and social security numbers have been compromised, this information could be used to cause significant damage to a victim's credit report. The urgency of notification should be balanced against any criminal investigation that may be underway.

In the event that a breach involves unauthorized access of the State of Illinois network and/or technology equipment and if the CMS Bureau of Communications and Computer Services ("BCCS") security team has not yet been notified of the incident, then BCCS should immediately be contacted for their assessment of the situation and input regarding the details of the incident and assessment of any further risk to the network environment. Immediately upon notice of an incident involving actual or potential breach, steps should be taken by CMS and/or the affected Agency (collectively called "Agency") responsible for the information. Several specific steps are provided below.

1. Notification to the appropriate law enforcement entity of an incident. Local, state and possibly federal law enforcement should be contacted depending upon the circumstances; (stolen laptop, unauthorized access to data network, stolen documents etc.). Agency should maintain ongoing dialog with law enforcement regarding the potential of containment, recovery and/or a determination of when an actual breach occurred in preparation for making a notification decision. Determining a value for the information potentially stolen, if any, may be important information for some law enforcement entities.

2. Agency should closely review the current version of the Personal Information Protection Act 815 ILCS 530/ to determine if there was in fact a "breach of the security of the system data" as defined by the Statute and understand and take appropriate steps to be in compliance with the Statute. Agency is advised to consult in house legal counsel to confirm its interpretation of the Statute.

3. Prepare for notification per the Statute:

    a. Section 530/12 (d) Requires state agencies to notify consumer reporting agencies if a breach requires an agency to notify more than 1,000 persons; There are three main credit reporting agencies to be notified;
    b. Section 530/25 requires state agencies to submit a report to the General Assembly within 5 business days of the discovery or notification of a breach of security of the system data or written material (read the Statute carefully for specific requirements of the notification);
    c. Notification must be made to the individual(s) affected by the breach per the Statute;

d. Section 530/10 (b-5) allows the notification to be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation. Agency should specifically ask law enforcement if they plan to make such a written request as quickly as possible and prior to any notification. If law enforcement does request Agency to delay notification due to the possible interference with the investigation, Agency should request a statement to that effect in writing from the law enforcement entity conducting the investigation;

4. Notification should be drafted so as to balance the need to timely provide the proper level of information regarding the breach that informs those affected per the requirements of the Statute and also to refrain from providing too much information that would potentially create further security issues or interfere with any criminal investigation(s). To that end, law enforcement and the BCCS security team should be consulted regarding the content of the notification prior to its release.

5. If a criminal investigation is underway, the notification letter should refer to the existence of an ongoing investigation and specifically to the investigation or police report number if applicable. The notification should direct those affected not to contact local law enforcement unless they have specific information about the crime itself and not simply to inquire about their own potential identify theft.

6. Those affected should be directed to inform the credit reporting agencies that an investigation is underway, and to provide the police report number upon request. The police report may be used as evidence against potential unauthorized purchases and also to possibly avoid any associated charges should the individual decide to request that a fraud alert be placed on their accounts.

7. Those who discover that their information has been misused are encouraged to file a complaint with the FTC at their web site www.consumer.gov/idtheft where current information about identify theft is also available. The web site also contains steps individuals can take to guard against and deal with identity theft.

8. Sample notification letters that address the above are available for use. One sample letter is attached to this procedure document.

9. A contact person should be designated within the Agency (or one each if multiple agencies are involved) for coordinating the response effort. An individual should also be designated to be the point of contact for releasing information when determined to be appropriate depending upon the specific circumstances of the incident. Agency Public Relations should begin preparing for items such as press inquiry response, working on the establishment of a set of FAQ's and to make determinations regarding who will field the high volume of potential calls, possibly setting up a call center to handle those calls.

10. A Determination should be made whether an internal investigation should be conducted with regard to the incident in case there is any possibility that an employee could be involved in the breach.

Once Agency completes statutory notification requirements, Agency should take the necessary steps to complete a follow up action plan that 1) Identifies potential or actual causes of the breach, and 2) Identifies measures to be taken that prevent the repeating of actions or inactions that contributed to the breach of the security of the system data.

Sample Letter:

Dear XXXXX,

We are writing to you because of a recent security incident at [name of organization]. [Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.]

To protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.] Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you visit the Web site of the [Federal Trade Commission at www.consumer.gov/idtheft]. If there is anything [name of your organization] can do to assist you, please call [toll-free phone number].

[Closing]