SAIC
From Science to Solutions

FACSIMILE TRANSMITTAL SHEET

TO:	FROM:
New Hampshire Attorney General	Amy L. Carlson
COMPANY:	DATE:
Department of Justice	12/9/2008
FAX NUMBER:	TOTAL NO. OF PAGES INCLUDING COVER:
603.271.2110	3
PHONE NUMBER:	SENDER'S CONTACT NUMBER:
603.271.3658	Phone: 206-370-5896 (Scott David for Amy Carlson)
RE:	YOUR REFERENCE NUMBER:
Notice of Data Security Incident	0324248-00001

☐ URGENT ☑ FOR REVIEW ☐ PLEASE COMMENT ☐ PLEASE REPLY ☐ PLEASE RECYCLE

NOTES/COMMENTS

Pursuant to the New Hampshire Right to Privacy Act, § 359-C:20 *et seq*, I am hereby notifying you of a data security incident involving one New Hampshire resident. SAIC has provided notice on December 8, 2008 to this individual through written notice, a copy of which is attached for your reference.

If you require any additional information or if you should have any further questions regarding this notification, please do not hesitate to contact me at:

Science Applications International Corporation
1710 SAIC Drive, M/S 3-5-9, McLean, VA 22102
(703) 676-6397 Phone
(703) 448-7732 Fax
amy.l.carlson@saic.com
www.saic.com

Amy Carlson
Chief Privacy Officer and
Vice President for Legal

AMY L. CARLSON
CHIEF PRIVACY OFFICER
1710 SAIC DRIVE, M/S 3-5-9 MCLEAN VA 22102
(703) 676-6397 (O) (703) 448-7732 (F)
AMY.L.CARLSON@SAIC.COM

[Individual Name/Home Address]
[Date]

This letter is to notify you of a potential compromise of your personal information, including your name and social security number, date of birth, home address, home phone number and clearance level and possibly other personal information necessary to complete government security clearance questionnaires (e.g., SF-85P or SF-86). We collected this information from you to provide it to the U.S. Government either to enable you to visit a government facility or to assist you in obtaining or updating your government clearance.

Our Security personnel routinely receive information regarding malicious software from industry partners. This process led to the recent discovery on October 28, 2008 of malicious software designed to provide backdoor access on a computer used to process your security clearance or visit request. Unfortunately, due to the nature of this malicious software, it avoided our standard cyber security precautions which include using industry-leading software for virus and spyware detection, intrusion detection systems, and firewalls. To help detect and prevent similar attacks, we keep pace with industry best practices and software, we continue to work with our industry partners and we are implementing Trusted Desktop, which removes elevated privileges from users.

We have communicated with Defense Security Information Exchange and the Federal Bureau of Investigation regarding this malicious software, and we have sought evidence regarding whether the malicious software was used to access your personal information. To date there is no indication that any of your personal data was accessed. As there is a potential that it could have been accessed, we recommend that you take precautionary measures, including the actions further detailed in Exhibit A attached to this letter.

We apologize for any inconvenience and concern that this situation may cause. Should you have any questions regarding this notice, including questions regarding your particular record, please do not hesitate to contact our Chief Privacy Officer, [_____], by phone at [_____], e-mail at [_____] or by mail at 1710 SAIC Dr., M/S 3-5-9, McLean, VA 22102.

Sincerely,

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION

[_____]
Business Unit General Manager
Operations, Intelligence & Security Business Unit

EXHIBIT A

IDENTITY THEFT PREVENTION INFORMATION

FTC: You may take steps to protect yourself against potential misuse of data that has been the subject of a data security incident. The Federal Trade Commission discusses several steps, including obtaining and reviewing your credit report, filing a "fraud alert" and requesting a "credit freeze". The most current and detailed information is available online (for answers to the questions below, see http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html), but if you are not able to access the linked material, you may also contact the FTC by mail at Federal Trade Commission, CRC-240, Washington, D.C. 20580, or by toll-free number, 1-877-FTC-HELP (382-4357) or 1-877-ID-THEFT (438-4338). You may also contact SAIC's Chief Privacy Officer, Amy Carlson, at 703-676-6397, amy.l.carlson@saic.com or 1710 SAIC Drive, M/S 3-5-9, McLean, VA 22102:

1. What are the steps I should take if I'm a victim of identity theft?
2. What is a fraud alert?
3. What is a credit freeze?
4. Should I apply for a new Social Security number?
5. What is an identity theft report?
6. What do I do if the police only take reports about identity theft over the Internet or telephone?
7. What do I do if the local police won't take a report?
8. How do I prove that I'm an identity theft victim?

Fraud Alert: A fraud alert tells creditors to take reasonable steps to verify your identity, including calling you before opening new accounts or changing your existing accounts. A fraud alert may be placed or removed at no cost to you. An initial fraud alert stays active for 90 days. To request a fraud alert, you will need to contact one of the following credit reporting agencies (see the FTC materials for further details). The credit reporting agency is required to notify the other two credit reporting agencies, who will also place a fraud alert on your credit file. You will then receive letters from all of them with instructions on how to obtain a free copy of your credit report from each.

Experian:	1-888-397-3742; www.experian.com; P.O. Box 9532, Allen, TX 75013
Equifax:	1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
TransUnion:	1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

If you observe evidence of attempts to open fraudulent accounts and you have a copy of a police report reporting that you are experiencing identity theft, then you may also request a 7-year fraud alert. Be aware that placing a fraud alert does not always prevent new accounts from being opened or prevent a takeover of your existing accounts, so you should monitor any alerts sent to you by the credit monitoring services. Also, be aware that a company may not be able to immediately extend credit to you if your identity can not be verified at the time you are applying for credit. You should consider providing a mobile telephone number when placing any fraud alert if you have one.

Monitor Credit Reports and Accounts: When you receive your credit reports, you should look them over carefully and consider taking the steps recommended by the FTC. For example, look for accounts you did not open. Additionally, look for inquiries from creditors that you did not initiate. And finally, look for personal information that you do not recognize. Also, you should monitor your accounts for suspicious activity. If you see anything you do not understand, call the credit reporting agency or provider of your account at the telephone number on the credit report or account statements. If you do find suspicious activity on your credit reports, you may call your local police or sheriff's office and may be able to file a police report of identity theft and obtain a copy of the police report. Potentially, you may need to give copies of the police report to creditors to clear up your records. You may also make a report to the FTC.

Obtain Free Credit Reports: Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report regularly for at least the next one to two years. Each of the three credit reporting agencies is required to provide you with a free credit report, at your request, once every 12 months. You may visit www.annualcreditreport.com, the only Web site authorized by Equifax, Experian and TransUnion for this purpose, to find out more. This website also provides instructions for making a request by phone (1-877-322-8228) or by mailing a request on a form supplied at the site and sending it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.