

**UNITED STATES
SECURITIES AND EXCHANGE COMMISSION**

Washington, D.C. 20549

FORM 8-K

**CURRENT REPORT
Pursuant to Section 13 OR 15(d) of
The Securities Exchange Act of 1934**

Date of Report: July 20, 2007

SAIC, Inc.

(Exact Name of Registrant as Specified in its Charter)

Delaware

(State or Other Jurisdiction of Incorporation)

001-33072

(Commission File Number)

10260 Campus Point Drive, San Diego, CA
(Address of Principal Executive Offices)

20-3562868

(I.R.S. Employer Identification No.)

92121

(Zip Code)

(858) 826-6000

(Registrant's Telephone Number, Including Area Code)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

- Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)
 - Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)
 - Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))
 - Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))
-

Item 8.01 Other Events.

On July 20, 2007, SAIC issued a press release describing actions it has taken to mitigate lapses by SAIC in data security relating to personal information processed by SAIC under several health care contracts for military service customers. A copy of the press release is furnished as Exhibit 99.1 to this report.

Item 9.01 Financial Statements and Exhibits.

(d) Exhibits

<u>Exhibit Number</u>	<u>Description</u>
99.1	Press Release dated July 20, 2007 issued by SAIC, Inc.

SIGNATURE

Pursuant to the requirements of the Securities Exchange Act of 1934, the Registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

(Registrant)

SAIC, INC.

Date: July 20, 2007

By: /s/ DOUGLAS E. SCOTT

Douglas E. Scott

Its: Executive Vice President

General Counsel and Secretary

FOR IMMEDIATE RELEASE

SAIC ADDRESSES POSSIBLE DATA COMPROMISE

(SAN DIEGO and MCLEAN, VA) July 20, 2007 – Personal information of certain uniformed service members, family members and others was placed at risk for potential compromise while being processed by SAIC under several health care data contracts for military service customers, the company said today.

SAIC remedied the security lapses upon learning of them and began working with the customers to mitigate any potential impact. Forensic analysis has not yielded any evidence that any personal information was actually compromised; however, the possibility cannot be ruled out. SAIC is notifying approximately 580,000 households, some with more than one affected person.

“We deeply regret this security failure and I want to extend our apologies to those affected by it,” Chairman and CEO Ken Dahlberg said. “We are concerned about the inconvenience and risk of potential compromise of personal information this may cause. The security failure is completely unacceptable and occurred as a result of clear violations of SAIC’s strong internal IT security policies. In this instance, we did not live up to the high level of performance that our customers have learned to expect and demand from us. We let down our customers and the service members whom we support. For this, we are very sorry.”

The information was stored on a single, SAIC-owned, non-secure server at a small SAIC location, and in some cases was transmitted over the Internet in an unencrypted form. The contracts were with customers in the Departments of the Army, Navy, Air Force and Homeland Security. The work was being done in connection with TRICARE, the health benefits program for the uniformed services, retirees and their families. The personal information at risk varies by individual, but could include combinations of names, addresses, Social Security numbers, birth dates, and/or limited health information in the form of codes.

The company is working closely with its government customers to mitigate any potential inconvenience or harm the possible compromise of personal information may cause. SAIC retained Kroll, Inc., a leading identity theft detection and mitigation firm, to provide services to affected individuals, including an Incident Response Center with extended hours, information resources, and credit and identity restoration services for any victims of related identity theft. These services will be provided at no cost to the government or the affected persons. The pre-tax cost of these services, which will be included in SAIC's financial results of operations for the three months ending July 31, 2007, is estimated to be in the range of \$7 million to \$9 million, excluding costs for credit restoration services if any related identity theft occurs.

"Our focus is on offering services and support to those who may be affected by the potential compromise of their information," according to Arnold Punaro, Executive Vice President, the company official leading the support effort.

The company has responded to this situation in a comprehensive way by taking the following actions:

- conducted a detailed forensic analysis of the server and data, which included assistance from some of the company's and the government's top experts in computer security;
- launched an internal investigation using outside counsel to determine exactly how this security failure occurred and placed a number of employees on administrative leave pending the outcome of the investigation;
- established a company-wide task force to ensure that the company responsibly addresses any adverse impact on the company's customers and any affected individuals;
- initiated a systematic, company-wide assessment to assure that such lapses do not exist elsewhere in the company and determine whether any changes in policy, methods, tools and monitoring are needed to make sure that such a lapse does not recur.

SAIC is a leading provider of scientific, engineering, systems integration and technical services and solutions to all branches of the U.S. military, agencies of the Department of Defense, the intelligence community, the U.S. Department of Homeland Security and

other U.S. Government civil agencies, as well as to customers in selected commercial markets. With more than 44,000 employees in over 150 cities worldwide, SAIC engineers and scientists solve complex technical challenges requiring innovative solutions for customers' mission-critical functions. SAIC had annual revenues of \$8.3 billion for its fiscal year ended January 31, 2007.

SAIC: FROM SCIENCE TO SOLUTIONS™

###

Statements in this announcement other than historical data and information constitute forward-looking statements that involve risks and uncertainties. A number of factors could cause our actual results, performance, achievements or industry results to be very different from the results, performance or achievements expressed or implied by such forward-looking statements. Some of these factors include, but are not limited to, the risk factors set forth in SAIC's Annual Report on Form 10-K for the period ended January 31, 2007, and such other filings that SAIC makes with the SEC from time to time. Due to such uncertainties and risks, readers are cautioned not to place undue reliance on such forward-looking statements, which speak only as of the date hereof.

Contact: Connie Custer, McLean Melissa Koskovich, McLean
 703-676-6533 703-676-6762
 custerc@saic.com koskovichm@saic.com

 Clayton Callihan, McLean
 703-676-6065
 callihanc@saic.com