Information Technology Services

One Washington Square
San Jose, CA 95192-0013
Voice: 408.924.7862
Fax: 408.924.1018

Jaime Sanchez
Director Network Services/ISO

Frank Reyes, Institutional Review Specialist
U.S. Department of Education, Federal Student Aid
50 Beale Street, Suite 9800
San Francisco, CA 94105-1863

RE: Data Security Breach
OPE ID Number: 00115500

Dear Mr. Reyes:

This letter is in response to the letter received from the Board of Education on July 30th, 2012. The response is in reference to the Data Security Breach OPE ID Number: 00115500 request.

On June 26th, 2012 Associated Students (A.S.) was approached by the news media that one of their servers had been hacked and information posted online. At around 10am I was notified of the breach with Associated Student's customer facing website and started working with A.S. to determine the extent of the breach.

We discovered that the initial probing started on June 21. Data harvesting started on June 22nd around 10 PM and continued to about 11:30 AM of the morning of June 23rd. The harvested data was hosted on **as.sjsu.edu** in several databases. Even though the majority of the harvested data was not classified as confidential level one data it did contain names, addresses, phone numbers and emails. The level one data included potentially 27 social security numbers and 218 driver's license numbers.

The social security numbers were not requested in any form by Associated Students but were rather inserted by the end user instead of inserting their student id or SJSUID. Some of these social security numbers belonged to Associated Students student employees. Again, they used their social security number instead of their student id when conducting testing of systems.

The hacker that breached the server used SQL Injections to harvest the data. This was confirmed by reviewing the server logs. We provided the source IP Addresses to campus police (SJSU UPD Case#SG1200853) who has forwarded to the FBI for further investigation. Appropriate measures have been taken to address the vulnerability. In addition, all confidential level one data has been removed from the server.

Associated Students mailed 223 notification letters to those individuals whose social security number or driver's license number was disclosed.
Of those, 218 were Breach Letters and 5 were SSN Breach Letters. As of August 18th, 2012 letters were returned as undeliverable; all 18 of them drivers licenses.

There were 22 emails sent with SSN Breach Letter. As of August 18th, 2012, 10 of the 22 email addresses were invalid or no longer in use and were bounced back. Associated Students does not have U.S. mail addresses for these users. Associated Students also cannot validate if all these users entered valid SSNs.

The following steps have been taken to strengthen its current procedures to safeguard Personally Identifiable Information (PII).

1.) Database cleanup and removal of unneeded data is completed. All potentially sensitive data that has been identified was changed to a value of 9 x (xxxxxxxxxx). All data that was no longer needed will be deleted.

    Databases:

    - Lrp
    - Lrp_databse (had DL numbers from the students who borrowed laptops)
    - Test (test db where students enter their own personal sensitive data in testing process)
    - Timetest (test db where students enter their own personal sensitive data in testing process)
    - Vjmehta (test db where students enter their own personal sensitive data in testing process)
    - Vjmehta1 (test db where students enter their own personal sensitive data in testing process)
    - Stickerdb (the largest list of names and student IDs)
    - Silentauction (old 2003 application with user generated username and passwords specific for this one time application)
    - Ascr_registration (2nd largest list of names and IDs)

2.) Restricted access to webpages that submit queries to databases is completed. Pages that have been restricted.

    - /ascsc/index.jsp
      /ascr/index.jsp
      /ascontact/index.jsp
      /asdocs/index.jsp
      /ase/index.jsp
      /asevents/index.jsp
      /asgov/index.jsp
      /asgsc/index.jsp
      /ashouse/index.jsp
      /asjobs_new/index.jsp
      /aslogos/index.jsp
      /aspg/index.jsp
      /asps/index.jsp
      /asts/index.jsp
      /cccac/index.jsp
      /intdocs/index.jsp
      /sits/index.jsp

3.) Updated code on web pages to prevent SQL injection.

    - asts/index.jsp, asts (carpool form), cccccac (volunteer form),

Campu req form

4.) Reviewing and updating code for SQL injection vulnerabilities in other web pages code.

Date of completion: Still TBD. We are in the process of actually recoding all the forms on the website one form at a time. It was not possible just to change a few strings of code since the code was written without these vulnerabilities in mind. This process is ongoing and will take months to complete every application and form. All unnecessary forms have been removed from the website so that less recoding needs to be done and it will limit the number of vulnerabilities.

Further improvements to prevent vulnerabilities for as.sjsu.edu web server:

5.) After finding the SQL injection or host injection issue(s) that deemed the web site vulnerable, there will be further examination regarding cross site scripting (XSS) as well.

6.) We will be isolating authentication accounts for applications. We will assign individual authentication accounts for each application to isolate access to specific databases per application. This will take some time as the current structure shares a database connection file. Individual connection files will be created and code will reflect that specific individual connection file.

7.) We will be patching our Sun Java Web Server/Oracle iPlanet Web server from 7.0U3 to the latest 7.0.15.

We are in the process of working with the CSU Chancellor's Office to deploy additional vulnerability tools to scan for Personally Identifiable Information across our server and desktop infrastructure. In addition, we are reviewing solutions for full disk encryption for all University owned equipment.

If you have any questions, please call Jaime Sanchez at (408)924-7862.

Sincerely,

Jaime Sanchez
Sr. Director Network Services/ISO