SPENCER BACHUS
6TH DISTRICT, ALABAMA

COMMITTEE:
FINANCIAL SERVICES,
RANKING REPUBLICAN MEMBER

Congress of the United States
House of Representatives
Washington, DC

2246 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-4921

1900 INTERNATIONAL PARK DRIVE
SUITE 107
BIRMINGHAM, AL 35243
(205) 969-2296

703 SECOND AVENUE NORTH
P.O. BOX 502
CLANTON, AL 35046
(205) 280-0704
http://www.house.gov/bachus

August 6, 2009

Via Facsimile (202-226-7514)

The Honorable Daniel Beard
Chief Administrative Officer
U.S. Capitol HB30
Washington, DC 20515-0001

Dear Mr. Beard,

On August 5, 2009, I was informed by Gary Warner, Director of Research in Computer Forensics at the University of Alabama at Birmingham and a constituent of mine, that it appeared my official House website had been "hacked". Gary Warner also identified other offices that were victims of the same attack. My staff immediately reached out to House Information Resources (HIR) to determine the cause of the "hack" and what appropriate action was necessary.

We were subsequently informed by staff of the CAO that the "hack" had occurred over the weekend of August 1-2, 2009. It is my understanding that your staff began working with the vendor for my website, GovTrends, shortly after the attack to determine the problem and resolve it.

While I appreciate the diligent work the staff of the CAO has done to resolve the issue, the incident has left several questions unanswered. Specifically, what is the procedure for notifying the victims of "hacks"? Only after questioning CAO staff were we told that we could expect information about the incident from GovTrends. As many as five days could have lapsed from when the "hack" occurred and when we would have been notified by GovTrends. It is my hope that your office will consider immediately informing Member offices of cyber attacks in the future rather than relying on outside vendors.

The Federal Information Security Management Act passed by Congress requires executive branch agencies to inform the US-CERT when an intrusion occurs against federal government systems. While Congress may be excluded from these required disclosure notices, what is the CAO policy regarding the disclosure of cyber attacks to law enforcement officials?

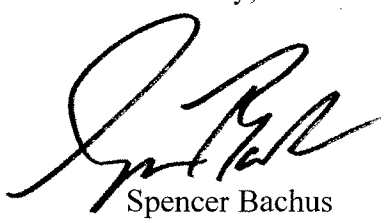
HIR informed my office that they do not often pursue prosecution because there is no way to track down the criminals responsible for these acts. However, Gary Warner, through his research, was able to document a series of more than 700 attacks by this criminal, a US-based server he believes was used by this hacker to host his blog where he provides tutorials on "SQL Injection" attacks, and intelligence revealing the university where the suspected hacker studied

computer programming. GovTrends refused to provide copies of the logs of the intrusion and deferred to CAO. While GovTrends is speculating to the press that this was a simple password guess, they have referred us to HIR to get evidence supporting their speculation. Please provide copies of the web logs and evidence supporting GovTrends speculation so that we can determine how best to proceed.

GovTrends bills itself as a "...trusted web solutions vendor for commercial and government clients, including the United States Congress." It is my understanding the CAO works with vendors to ensure appropriate web security standards are met. Please provide an explanation of the vulnerability that allowed this situation to occur and what is being done to prevent it from happening again in the future.

It is extremely important that my constituents can trust that information provided to my office is kept confidential and secure. I look forward to your responses.

Sincerely,



Spencer Bachus
Member of Congress

STB/cws
cc: The Honorable Nancy Pelosi, Speaker of the House
The Honorable John Boehner, House Minority Leader
The Honorable Robert Brady, Chairman, House Administration Committee
The Honorable Dan Lungren, Ranking Member, House Administration Committee
The Honorable Wilson Livingood, Sergeant at Arms of the House