NEW YORK STATE SENATOR

Jeffrey D. Klein

Klein Reveals State National Guard Website Hacked

JEFFREY D. KLEIN February 12, 2005

Bronx, NY –The servers and websites of New York State agencies and authorities have been successfully hacked at least seventy-one times since 1999, according to a report by Senator Jeff Klein. The State Division of Military and Naval Affairs (DMNA), the State Education Department, the State Power Authority, several SUNY and CUNY campuses, and the State Department of Motor Vehicles were among many agencies whose security was compromised. Entitled **Tip of the Iceberg,** the report suggests the actual number of web intrusions is likely even greater, since many go undetected.

"Secure government computer systems are of vital importance, particularly in a post 9/11 environment," stated Senator Jeff Klein. "Emergency response-related agencies use web sites to disseminate information during emergencies. Terrorists may try to tamper with or disable the State's networks to amplify the effect of a physical attack."

That concern arose when a hacker broke into the server for the DMNA website last June. The website, which contains information about the activities of the National Guard, had its web pages deleted and replaced by postings created by the hacker. At that high level of access, the hacker could have copied or changed information stored on the server.

Another breach occurred in August, when a self-replicating computer virus of unknown origin crashed the network of the State Department of Education. A subsequent investigation by the State Police found that the virus had installed file transfer programs capable of stealing information stored on agency computers.

"There is information about sixteen million state residents in the state's computer systems," noted Klein. "If a security breach occurs, potential victims ought to be informed. The Assembly last year passed a bill to do just that -- I'm urging the State Senate and the Governor to approve that bill."

In the case of the Education Department attack, the virus was detected by the State's Intrusion Detection Network, which as of January of this year, only covered twenty of over sixty agency websites. Yet, the Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) failed to immediately notify other agencies about the attack, including many uncovered by the detection system. This is just one of several faults that the report levels at the CSCIC.

"Information Security Officers (ISOs) – agency level technology security personnel – are sometimes put in place prior to receiving the training necessary to do their job," added Klein. "The result is that the state has to depend on outside contractors to beef up their expertise – adding cost to the taxpayer and complicating security issues."

"We need to make reforms to our security infrastructure," concluded Klein. "We need more ISOs who are better trained. We need a comprehensive Intrusion Detection Network that will better protect our state computer systems. At the very least, we need to inform state residents when security is breached so that they will also be vigilant for identity theft or other related fraud."

-30-