February 26, 2015

PRESS RELEASE
FOR IMMEDIATE RELEASE

VIR-SEC: DHS Einstein Program Fails to Meet Best Practices, Focuses on Spying as Opposed to Security

WASHINGTON, D.C. — Vir-Sec, Inc., a cybersecurity company based out of Clearwater, FL, is responding to the news that the Department of Homeland Security's Einstein program is stalling due to questions over security, liability, privacy and cost.

The Einstein program, also known as E3A, is designed to protect federal computer networks from hackers and to block malicious Internet traffic before it reaches federal agencies. POLITICO reported in late February that negotiations over the implementation of the program were at a standstill due to concerns over who would be held liable if the system failed and didn't work.

POLITICO also reported that the program was stalling due to privacy concerns as to the extent DHS would be monitoring Internet traffic of ordinary citizens. Einstein E3A scans traffic to or from federal networks, analyzing for Internet addresses or specific coding signatures that are signs of malware at work. The latest version of the program was upgraded to alert system administrators and intercept malicious data and stop it.

Vir-Sec, however, is strongly warning the government that the Einstein program fails to meet best practices for protecting web applications and websites. Director of Government Affairs John Foti warned that not only is the federal government implementing a program it knows isn't best practices, but that giving liability protection to the security provider will only encourage mediocrity in implementation and practice.

"DHS is attempting to protect federal websites and web portals with an outdated and failed solution, and that could have consequences if anyone questions the validity of the Einstein program's practices," explained Foti. "Unless DHS can say that the Einstein program's standards can live up to Vir-Sec's standards, then the government and those associated with the Einstein program should be held liable."

Vir-Sec cited its SecureAxcess™ technology as the basis for best practices, stating that their technology has the ability to secure internal web-portals and web applications from public facing websites so that the internal access point is removed from a public facing website.

Vir-Sec explained that only DHS and federal employees should have access to federal web portals, including email and other web-based applications. SecureAxcess™ allows only known users to access secure data through a browser-less web application via the Internet. Therefore organizations can remove access to their internal networks from their public facing websites and leave only HTML text on a website for the public to see.

SecureAxcess™ would also eliminate any browser-based access to its web portals and applications, reducing the entire attack surface of federal portals and applications to only known users, meaning an individual would first have to physically infiltrate DHS in order to then access its web portals and applications.

Vir-Sec went on to say that they have more concerns over the Einstein program other than the E3A's program failure to meet best practices and liability for the program. Vir-Sec's also concerned with the program's scanning of Internet traffic to and from federal websites, which Foti has described as "Orwellian spying tactics" and said violated Americans' constitutional rights.

"The Einstein program would deploy Orwellian spying tactics in order to catch cyber criminals, clearly violating the Fourth Amendment by assuming every user that navigates to the government's public website is a bad actor," said Foti. "Citizens should not be subject to federal monitoring simply because they decide to use the Internet."

Privacy advocates have shared Vir-Sec's concerns since the new version of the Einstein program was announced, with many saying that their concerns are the reason why certain partners in the program may be seeking liability protection.

In addition, Vir-Sec is also questioning the pricing of the program, citing theirs costs to provide best practices in cybersecurity as the basis of their skepticism. "We could eliminate the threat of cyber-attacks DHS is trying to prevent for a fraction of the cost," said Foti. "Not only is the government not deploying best practices, but they are also paying more to deploy an inadequate cybersecurity solution."

CONTACT:

Chris Murphy
Founder, Chairman & CEO
Vir-Sec, Inc.
chris.murphy@vir-sec.com

John Foti
Director
Government Affairs
Vir-Sec, Inc.
Email: JFoti@Vir-Sec.com

###