Spotlight

Fred Donovan

Cyberspace is fundamentally a civilian space, and government has a role to help protect it, in partnership with responsible partners across the economy and across the globe

Janet Napolitano

Obstacles Facing the US Cybersecurity Initiatve

Although the US government is paying more attention than ever to the issue of cybersecurity, the recent battles in Washington over budgets and austerity measures mean that funding could potentially dry up in an instant. Fred Donovan surveys the experts to get their take on where the nation's cybersecurity program is heading

It has been more than three years since President Bush signed the presidential directive to implement the Comprehensive National Cybersecurity Initiative (CNCI). While details of the plan remain classified, his successor, President Obama, released a summary of the CNCI that identifies 12 government initiatives intended to beef up cybersecurity for the US government, as well as promote public-private sector cybersecurity efforts.

The three main goals of the CNCI are: 1) to establish defenses against immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events and developing a capability to respond rapidly to shore up vulnerabilities and prevent network intrusions; 2) to enhance US counterintelligence capabilities and increase the security of the IT supply chain; and 3) to strengthen the future cybersecurity environment by expanding cyber education, research and development efforts, and strategies to deter hostile or malicious activity in cyberspace.

The Cyberspace Policy Review, undertaken by President Obama, endorsed the CNCI and recommended that an Executive Branch Cybersecurity Coordinator be named to work with federal, state, and local governments – as well as the private sector – to strengthen the nation's cybersecurity posture. In 2009, Obama named Howard Schmidt, a former cybersecurity advisor to Bush, as his cybersecurity coordinator.

Infosecurity asked cybersecurity experts – including current and former federal government officials – and cybersecurity vendors to assess the progress being made under the CNCI three years out.

A Move in the Right Direction

Hord Tipton, executive director of the non-profit IT security trade group (ISC)[2] and former chief information officer (CIO) of the US Department of the Interior, said that the US government has made "substantial progress" in establishing defenses against threats and responses to network intrusions, particularly with the development and deployment of the Einstein intrusion detection and prevention systems. "We were the second cabinet-level department to join in and take advantage of Einstein", he shares. "We in Interior actually started Einstein at Level 1, and now it is at Level 3", says Tipton, who was CIO at Interior from 2002 to 2007.

Einstein 1 and 2 focused on intrusion detection for US government networks, while Einstein 3, which is being deployed this year, is designed to automatically detect and disrupt malicious network activity.

Download English Version:

https://daneshyari.com/en/article/458425

Download Persian Version:

https://daneshyari.com/article/458425

Daneshyari.com