

US boots up new unified cybersecurity center

October 30 2009, by Chris Lefkow



US Homeland Security Secretary Janet Napolitano joins staff members and members of the U.S. Congress at the ribbon-cutting ceremony of the new U.S. Computer Emergency Readiness Team/National Cybersecurity and Communications Integration Center facility October 30, 2009 in Arlington, Virginia.

US Homeland Security Secretary Janet Napolitano cut the ribbon on Friday on a state-of-the-art unified command center for government cybersecurity efforts.

The National Cybersecurity and Communications Integration Center (NCCIC) brings together various government organizations responsible for protecting cyber networks and infrastructure and private sector partners.

"This will be a 24/7, 365-day-a-year facility to improve our national efforts to prepare and respond to threats and incidents affecting critical

information technology and communications infrastructure," Napolitano said.

She said the NCCIC will serve as the "central repository" for the cyber protection efforts of the civilian side of the federal government and its private sector partners.

Attending the ribbon-cutting ceremony for the NCCIC was the head of the US military's "cyber command," Lieutenant General Keith Alexander, director of the super-secret National Security Agency (NSA).

The high-security new NCCIC facility is located in an Arlington, Virginia, office building and includes a long narrow room dominated by giant wall-mounted video screens displaying maps and threat data. Facing the screens are dozens of computer work stations with multiple screens.

"Securing America's cyber infrastructure requires a coordinated and flexible system to detect threats and communicate protective measures to our federal, state, local, and private sector partners and the public," Napolitano said.

"Consolidating our cyber and communications operations centers within the NCCIC will enhance our ability to effectively mitigate risks and respond to threats," she added.

NCCIC combines two Homeland Security operational organizations: the US Computer Emergency Readiness Team (US-CERT) and the National Coordinating Center for Telecommunications (NCC).

US-CERT is a public-private partnership aimed to protecting and defending cyber infrastructure while the NCC is the operational arm of the National Communications System.

NCCIC will also integrate the National Cybersecurity Center (NCSC), which coordinates operations among the six largest federal cyber centers.

Napolitano, whose department has received the green light to hire up to 1,000 cybersecurity experts over the next three years, stressed the private sector participation in the NCCIC, noting they will have "offices in the same space."

US-CERT currently partners with a number of private sector companies such as telecommunications firms and others in monitoring cyber threats.

The opening of the NCCIC was the culmination of what has been dubbed "National Cybersecurity Awareness Month."

No single agency is currently charged with ensuring government information technology security and lawmakers have called for creating a powerful national cybersecurity advisor reporting directly to the president.

President Barack Obama has made cybersecurity a top priority and announced in May that he would name a "cyber czar" to defend against criminal, espionage and hacker attacks on US government and private computer networks.

Obama has not yet named the "cyber czar" but the 2010 Homeland Security Act that he signed on Wednesday included 397 million dollars for cybersecurity.

US government websites come under attack on a daily basis, according to the Department of Homeland Security, with the threats ranging from teenage hackers to criminal gangs to foreign governments.

(c) 2009 AFP

Citation: US boots up new unified cybersecurity center (2009, October 30) retrieved 19 April 2024 from <https://phys.org/news/2009-10-boots-cybersecurity-center.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.