THE HOMELAND SECURITY SECRETARY'S MORNING CLIPS

MONDAY, JULY 25, 2011 5:00 AM EDT

[redacted]

[redacted]

Senior US Cybersecurity Official Resigns (AFP)

AFP, July 26, 2011

WASHINGTON — A Department of Homeland Security (DHS) official responsible for defending US government networks against cyberattacks resigned on Monday.

Randy Vickers stepped down as director of the US Computer Emergency Readiness Team (US-CERT), the operational arm of the DHS's National Cyber Security Division.

Vickers' resignation was announced in an email to staff from Bobbie Stempfley, the DHS's acting assistant secretary for cybersecurity and communications.

A DHS official declined to provide an explanation for his departure saying the department does not discuss personnel matters.

But Information Week, which first reported Vickers' resignation, noted that it followed a string of cyberattacks on US government networks by hacker groups such as Anonymous and Lulz Security.

Lulz Security has claimed responsibility during the past few weeks for attacks on the websites of the Central Intelligence Agency, the US Senate, the Arizona Department of Public Safety and others.

US Deputy Defense Secretary William Lynn said earlier this month that a foreign intelligence service swiped 24,000 computer files from a US defense contractor in March in one of the largest ever cyberattacks on a Pentagon supplier.

The Washington-based US-CERT is responsible for the protection of US government computer networks and also cooperates on cybersecurity with the private sector and state and local authorities

Stempfley, in the email obtained by AFP, said Vickers' resignation was effective on Friday. She said he would be replaced by US-CERT deputy director Lee Rock until a new director is named.

"Lee has been the deputy director for US-CERT for over a year and we are confident that our organization will continue its strong performance under his leadership," Stempfley said. "We wish Randy success in his future endeavors."

[redacted]

US-CERT Director Leaves Abruptly (INFOWEEK)

By Elizabeth Montalbano

Information Week, July 25, 2011

The director of the agency that protects the federal government from cyber attacks has resigned abruptly in the wake of a spate of hacks against government networks.

U.S. Computer Emergency Readiness Team (US-CERT) director Randy Vickers resigned his position Friday, effective immediately, according to an e-mail to US-CERT staff sent by Bobbie Stempfley, acting assistant secretary for cybersecurity and

communications, and obtained by InformationWeek. A Department of Homeland Security (DHS) spokesperson confirmed the email was authentic.

The DHS has not provided a reason for Vickers' sudden departure and the spokesperson, who asked to remain anonymous, declined to discuss the matter further. Vickers served as director of US-CERT since April 2009; previously, he was deputy director.

Current US-CERT deputy director Lee Rock will serve as interim director until the DHS names a successor for Vickers, according to the email.

"We are confident that our organization will continue its strong performance under his leadership," Stempfley wrote, adding that the agency wishes Vickers success in future endeavors.

Vickers' departure comes at a critical time for the organization, as federal networks have come under a barrage of attacks lately by a series of hacker groups--including Anonymous, LulzSec and AntiSec--that specifically are targeting government networks.

In the last month and a half, federal organizations that have experienced attacks include the Navy, the FBI, and the CIA. Federal contractors that handle sensitive and confidential government information also have been the targets of hackers, including Booz Allen Hamilton and IRC Federal.

In response to those attacks last week, US-CERT issued a comprehensive new set of security recommendations for federal agencies and organizations to follow in the hope of preventing future intrusions.

US-CERT is a division of the DHS responsible for responding to and defending against cyber attacks for the federal government's IT infrastructure. It also is in charge of sharing information and collaborating with state and local governments, as well as the private sector, to protect critical infrastructure in the United States.

One of the organization's jobs is to keep track of attacks on federal networks and compile a list of them by type and number for a yearly report released by the Office of Management and Budget. The report helps the feds better understand where vulnerabilities lie as part of an overall cybersecurity strategy that has become increasingly important in the last several years. What industry can teach government about IT innovation and efficiency. Also in the new, all-digital issue of InformationWeek Government: Federal agencies have to shift from annual IT security assessments to continuous monitoring of their risks. Download it now. (Free registration required.)

[redacted]

Top US Cybersecurity Official Quits (YAHOO)

By Trevor Mogg

Yahoo News, July 26, 2011

The US Computer Emergency Readiness Team (US-CERT) isn't looking quite so ready at the moment as its director has just quit. US-CERT, part of the Department of Homeland Security (DHS), is charged with the task of protecting US government agencies and networks from cyberattacks.

According to an Information Week report on Monday, the former DHS official, Randy Vickers, left his post at the end of last week. He'd been in the position since April 2009.

The report said that in an email announcing the news, sent to staff by DHS's acting assistant secretary for cybersecurity and communications Bobbie Stempfley, no explanation was given as to why Vickers had decided to resign.

In the past few months, however, a number of government agencies have been hit by hackers in a string of embarrassing cyberattacks.

In June the LulzSec hacker group hit the CIA website with a denial-of-service attack, and shortly before that the website of InfraGard, a non-profit organization that serves as a partnership between the FBI and private business, was hit by the same group.

In the same month, officials working at the White House were at the center of a phishing attack where hackers, believed to be located overseas, tried to trick users of Gmail into giving away their passwords.

Federal contractors dealing with confidential government information have also been targeted by hackers – earlier this month Booz Allen Hamilton lost 90,000 email addresses and passwords after a security breach orchestrated by another hacking group, Anonymous.

On its website, US-CERT cites its mission as "to improve the nation's cybersecurity posture, coordinate cyber information sharing and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans."

US-CERT deputy director Lee Rock will fill Vickers' position until a new director is announced.

In the email sent to staff on Friday, Stempfley wrote: "Lee has been the deputy director for US-CERT for over a year and we are confident that our organization will continue its strong performance under his leadership."

Describing the performance as "strong" may be scoffed at by some observers, but there's little doubt that in the world of cybersecurity, this must be one of the toughest jobs going. Whichever brave soul takes on the role full-time, hopefully they'll have been able to learn a lot from the recent string of cyberattacks.