



[back](#)

DHS relooking at how to classify cyber incidents

By [Jason Miller](#)
Executive Editor
FederalNewsRadio

The Homeland Security Department's U.S. Computer Emergency Response Team (U.S.-Cert) will make suggestions about how to change the way the government tracks cyber attacks.

The current set of categories is seven-years-old and has not kept up with the changing cybersecurity environment, says Mischel Kwon, director of U.S.-Cert.

Kwon says the top two types of cyber attacks are not included in the statistics.

"The attacks that concern us the most are phishing and drive by Web attacks," she says. "This is where someone sends you a bad e-mail that looks like it comes from someone you trust, and you click on the link. The link sends you to a Web site and you download malware. These are the most prevalent types of attacks. They are hardest to detect and prevent, and are easiest for people with malicious intent to do."

Kwon adds that U.S.-Cert will submit its suggestions to the directors of agency network security operations center for approval later this year.

The new cyber categories U.S.-Cert is developing come as DHS released its 2008 statistics on federal civilian agency incidents. The Defense Department reports its incidents to the Joint Task Force for Global Network Operations (JTF-GNO).

In 2008, civilian agencies reported to U.S.-Cert some 7,000 more cyber incidents than the year before.

About 7,500 of these 18,050 incidents are under investigation, while agencies reported more than 3,700 improper usage events and more than 3,200 unauthorized accesses.

Kwon says these numbers do not tell the entire story of the state of federal cybersecurity.

"What is important to note about these numbers is the state of where we are in cybersecurity," she says. "In civilian agencies, it is just beginning and growing. Few agencies have active security operations centers and the numbers depict that because they seem low."

Kwon adds that more agencies are reporting incidents, and how they account for them has improved as well.

More agencies also are bringing security operations centers online to detect these incidents as a part of the Trusted Internet Connections (TIC) initiative. Under TIC, agencies are implementing the Einstein intrusion detection software and reducing the number of Internet access points.

"We see a big difference because of TIC," Kwon says. "There is a lot more technical support for agencies."

Kwon says the statistics give a general state of how agencies are doing in protecting their networks.

"We can't do much detailed analysis on those incidents," Kwon says. "I'm not sure they actually went down. I'm not sure how accurate the reporting is because it's done manually."

Kwon says through TIC, Einstein and security operations centers agency reporting should become more automated and therefore more accurate.

On the Web:

Only on FederalNewsRadio - [DHS cyber incidents report for 2008](#) (doc)

FederalNewsRadio - [White House calls for review of all cybersecurity plans, programs](#)

FederalNewsRadio - [Head of DHS cyber receives promotion](#)

FederalNewsRadio - [Cybersecurity workforce standards finalized](#)

DHS - [U.S.-Cert Web site](#)

(Copyright 2009 by FederalNewsRadio.com. All Rights Reserved.)