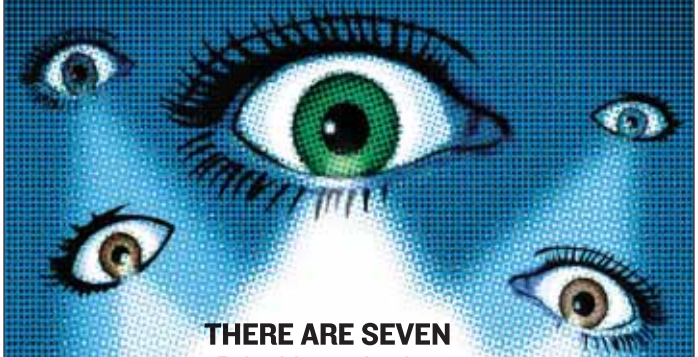
What to report and when



THERE ARE SEVEN Federal Agency Incident Categories categories for which agencies must report IT security incidents to U.S. CERT. The five that require the fastest reporting are:

CATEGORY 1, UNAUTHORIZED ACCESS

In this category an individual gains logical or physical access without permission to an agency network, system, application, data or other resource. Report within **one hour** of discovery. This includes personal information.

CATEGORY 2, DENIAL OF SERVICE

An attack that successfully prevents or impairs the normal functions of networks, systems or applications by exhausting resources. Report within **two hours** of detection if the successful attack is still ongoing, and the agency is unable to successfully mitigate activity.

CATEGORY 3, MALICIOUS CODE

Successful installation of malicious software that infects an OS or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus software. Agencies must report **daily or within one hour** of detection if widespread across the agency.

CATEGORY 4, IMPROPER USE

A person violates acceptable computing use policies. Report **weekly**.

CATEGORY 5, SCANS/PROBES/ATTEMPTED ACCESS

Any activity that seeks to access or identify a federal agency computer, open ports, protocols, service or any combination for later exploitation, but does not directly result in a compromise or denial of service. Report **monthly** or, if system is classified, within **one hour** of discovery.

Categories 0 and 6 deal with internal incidents that occur as part of testing or an investigation, and do not require reporting to U.S. CERT.