

# Federal Agency Incident Categories

Category	Name	Description	Reporting Timeframe
<b>CAT 0</b>	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
<b>CAT 1</b>	Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource	Within one (1) hour of discovery/detection.
<b>CAT 2</b>	Denial of Service (DoS)	An attack that <i>successfully</i> prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
<b>CAT 3</b>	Malicious Code	<i>Successful</i> installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been <i>successfully quarantined</i> by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
<b>CAT 4</b>	Improper Usage	A person violates acceptable computing use policies.	Weekly
<b>CAT 5</b>	Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
<b>CAT 6</b>	Investigation	<i>Unconfirmed</i> incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.