Internet Security

ALARM

Use of alarm systems in Sensitive Compartmented Information Facilities to ensure non-cleared personnel are under constant oversight to prevent unauthorized access to classified information

CRACKING

When an individual with extensive computer knowledge purposely breaches, bypasses internet security, or gains access to software without paying royalties

SCANNING

Communicating with a web application in order to identify potential security vulnerabilities in the web application and architectural weaknesses

INSIDER THREAT

A malicious threat to an organization that comes from the likelihood, risk, or potential that an insider will use their authorized access, wittingly or unwittingly, to do harm to the national security of the United States.

HACKER

A person who secretly gets access to a computer system in order to get and/or tamper information, cause damage, or otherwise illegaly comporises an electronic service or system

VIRUS

A malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected"