LEADS Daily Bulletin
August 15 2022

CJIS Security policy - Spam and Spyware Protection

Pursuant to the FBI CJIS Security Policy, Section 5.10.4.3, agencies shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.

For assistance with the CJIS Security Policy please contact the ISP CJIS Information Security Officer via email: ISP.LEADSISO@Illinois.gov

Operator's Initials	Date	Operator's Initials	Date	Operator's Initials	Date	Operator's Initials	Date	Operator's Initials	Date