# Cyber Defense

Defense Security Service
Office of Counterintelligence, Huntsville, AL

**Cyber Event of Interest:**

**December 15, 2010**

## Cyber events of Interest

Report insider initiated attacks against CDC automated information systems that appear to involve:

-Unauthorized sniffers

-Suspicious downloads of sensitive data

-Unauthorized modems

-Unexplained storage of encrypted data

-Anomalous work hours and or network activity

-Unexplained modification of network security-related operating system settings

-Unexplained modification of network security-security devices such as routers and firewalls

-Malicious code that attempts to establish communication with systems other that the one on which the code resides.

-Unexplained external physical network/computer connections

-Unexplained modification to network hardware

-Unexplained FTP servers on inside of security perimeter

-Unexplained hardware or software found on internal networks

-Network interface cards (NICs) that are set in a promiscuous/sniffer mode

-Unexpected open maintenance ports on network components

-Any unusual activity associated with network enables peripheral devices such as printer and copiers

-Any unusual or unexplained activity focused on transfer devices authorized for moving data across classification boundaries.

-Unexplained attacks appearing to originate from within the local network.

-Attacks against specific network devices (such as intrusion detection systems) originating internal to the local network.

-Unexplained scans for vulnerabilities originating internal to the local network

-Serious vulnerabilities remaining uncorrected after multiple notifications to the responsible individual to correct the problem

-Unusual interest in network topologies (firewall, security hardware/software Inter-site connectivity, trust relationships, etc)

-Unusual interest in penetration and/or vulnerability testing of the network.

-Unexplained hidden accounts or expected levels of privilege.

-Unauthorized attempts to elevate privilege

-Attempts to introduce software unapproved for the computing environment.

-Individuals with access displaying any of the following characteristics:

    -Undue affluence

    -Unexplained travel

    -Unexplained foreign contacts

    -Unwillingness to take vacation

    -Unwillingness to allow someone to assume their duties

    -Exploitable conduct

    -Abnormal behavior

    -Unexplained and/or extensive technical computer-related knowledge

-Report telephonic indicators of attacks against CDC automated information systems that appear to involve:

    -Unauthorized modem connections

    -Encrypted telephonic communications on lines not specifically identified as normally used for encrypted traffic

    -Excessive, unusual and/or unexplained computer connections over the telephone infrastructure to foreign countries (as identified by traffic analysis or other means)

    -Unexplained devices associated with the telephone infrastructure or the connections between the telephone and computing infrastructures.