SECULORE™

VoiceProducts
VOICE • VIDEO • DATA

New CJIS Requirements

Section 5.15, SI-2 Flaw Remediation

Satisfied by CJIS Assist

Assisted by CJIS Assist

[Existing] [Priority 1]

Control:

a) Identify, report, and correct system flaws;

b) Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c) Install security-relevant software and firmware updates within the number of days listed after the release of the updates;

- Critical – 15 days
- High – 30 days
- Medium – 60 days
- Low – 90 days; and

d) Incorporate flaw remediation into the organizational configuration management process.

Section 5.15, SI-4 System Monitoring

a) Monitor the system to detect:

- Attacks and indicators of potential attacks in accordance with the following monitoring objectives:
  - Intrusion detection and prevention
  - Malicious code protection
  - Vulnerability scanning
  - Audit record monitoring
  - Network monitoring
  - Firewall monitoring;
- Unauthorized local, network, and remote connections;

b) Identify unauthorized use of the system through the following techniques and methods: event logging (ref. 5.4 Audit and Accountability);

c) Invoke internal monitoring capabilities or deploy monitoring devices:

- Strategically within the system to collect organization-determined essential information; and
- At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d) Analyze detected events and anomalies;

Satisfied by CJIS Assist

Assisted by CJIS Assist

Section 5.19, RA-5 Vulnerability Monitoring & Scanning

a) Monitor and scan for vulnerabilities in the system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system are identified and reported;

b) Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

- » Enumerating platforms, software flaws, and improper configurations;
- » Formatting checklists and test procedures; and
- » Measuring vulnerability impact;

c) Analyze vulnerability scan reports and results from vulnerability monitoring;

d) Remediate legitimate vulnerabilities within the number of days listed;

- » Critical–15 days
- » High–30 days
- » Medium–60 days
- » Low–90 days; and

e) Share information obtained ...

f) Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.