SC.L2-3.13.14

System & Communications Protection

Voice over Internet Protocol

"Control and monitor the use of Voice over Internet Protocol (VoIP) technologies."

Objectives

[a]

Use of Voice over Internet Protocol (VoIP) technologies is controlled.

[b]

Use of Voice over Internet Protocol (VoIP) technologies is monitored.

Key Discussion Points

Control = Policy + Config: VoIP control requires an acceptable use policy AND technical configuration — encryption, strong credentials, and access controls must be actively configured.

Monitor the Logs: VoIP systems generate call logs — monitoring for anomalous call volumes, unauthorized registrations, and after-hours activity detects abuse and toll fraud.

Eavesdropping Risk: Unencrypted VoIP can be intercepted on any network segment the call traverses — conversations containing CUI are exposed without any action by the caller.

Includes Personal Apps: The control applies to all VoIP technologies in use — unsanctioned apps like WhatsApp or FaceTime used for work calls must be addressed in policy.

Assessment Methods

EXAMINE

System and communications protection policy; procedures addressing VoIP; VoIP usage restrictions; VoIP implementation guidance; system security plan; system design documentation; system audit logs; system configuration settings; system monitoring records.

INTERVIEW

System or network administrators; personnel with information security responsibilities; personnel with responsibilities for managing VoIP.

TEST

Organizational processes for authorizing, monitoring, and controlling VoIP; mechanisms supporting or implementing authorizing, monitoring, and controlling VoIP.

SC.L2-3.13.14

SYSTEM & COMMS PROTECTION — Voice over Internet Protocol

Plain English

What this control is really saying:

VoIP carries voice calls as network traffic — and like all network traffic, it can be intercepted, spoofed, or abused. An attacker can eavesdrop on an unencrypted VoIP call containing CUI, impersonate a trusted caller using caller ID spoofing, or abuse an unconfigured VoIP extension as an attack vector. This control requires a policy governing VoIP use and monitoring for unauthorized or insecure VoIP activity.

How it is used:

- The VoIP acceptable use policy defines authorized use cases, prohibited activities, and the process for provisioning new users — users sign the policy before VoIP access is granted.
- VoIP traffic is encrypted — the platform is configured to require TLS for signaling and SRTP for media, preventing eavesdropping on calls.
- VoIP system logs are sent to the log aggregator and reviewed as part of the regular log review process — anomalous call patterns and unauthorized access attempts generate alerts.
- Voicemail and phone system administration require strong passwords and MFA — default credentials are changed at deployment.

Real World Example

The Scenario

Acme Defense uses a cloud-based VoIP system for all business calls. The system is configured without encryption. Engineers regularly discuss CUI project details over VoIP calls with the DoD program office.

What the assessor finds

An assessor reviews the VoIP configuration and confirms signaling and media are unencrypted. VoIP traffic captured on the network reveals intelligible voice content from engineering discussions containing CUI design details. No monitoring exists to detect anomalous call activity.

SPRS Score Impact

3.13.14 carries a point value of 1. Unencrypted VoIP carrying CUI discussions is a passive interception risk on any network segment the traffic traverses — no user action is required for an attacker to collect intelligence from calls.

What Good Looks Like

VoIP acceptable use policy documented, traffic encrypted with TLS and SRTP, strong passwords and MFA on voicemail and admin interfaces, VoIP logs reviewed as part of regular monitoring, unapproved VoIP applications addressed in policy.

Common Gaps

What assessors actually find in the field:

✗ VoIP calls not encrypted

The VoIP system transmits voice calls without encryption — calls containing CUI can be intercepted on the network.

✗ No VoIP policy

VoIP is deployed and in use but no policy defines acceptable use, authorized configurations, or monitoring requirements.

✗ Default credentials in use

Voicemail passwords are still set to the carrier default — any caller who knows the extension can access voicemail without authorization.

✗ VoIP logs not monitored

VoIP system logs are generated but not reviewed — unauthorized registrations, toll fraud, and anomalous call patterns go undetected.

✗ Unapproved VoIP applications

Employees use personal VoIP applications (WhatsApp, Signal, FaceTime) for work calls — no policy addresses or controls these applications.