
# TSG Compliance in the Age of Softphones

Document #: CIS04092026
Revision #: 0.14
Date: 04.05.26

## 1. EXECUTIVE SUMMARY

Like many enterprises in industry, the federal government is undergoing a fundamental transformation in enterprise communications. Civilian, Defense and Intelligence Community (IC) agencies are shifting from legacy, hardware-centric telephony systems to software defined voice and collaboration solutions operating on both on-premise systems and cloud platforms. The exponential proliferation of users leveraging cloud-based collaboration started during the pandemic in 2020 as the government had to deliver voice, video, messaging, and data sharing services to users who no longer had their desk phones in front of them. This transition of mission demands drove the need for mobility, interoperability, and integration across distributed operational environments, where these services were delivered via software applications rather than discrete desktop instruments.

While this evolution to software-based collaboration enables significant operational flexibility and efficiency, it also introduces a different set of security challenges for environments governed by CNSSI 5000 and National Telecommunications Security Working Group (NTSWG) Telephone Security Group (TSG) requirements. Traditional TSG-compliant desk phones were engineered to provide deterministic, hardware enforced protections, particularly “on-hook security,” which ensures that audio cannot be transmitted when a device is in the idle state.

TSG phones deliver a layer of physical security by ensuring that the peripherals built into the phone (handset and speakerphone) or connected to it (headset) cannot be used to eavesdrop on conversations taking place near the phone when it is not in use. Enhancements to commercially available phones that make them TSG compliant include the addition of physical circuitry designed to disengage the peripherals until the user proactively presses the TSG button to engage them when needed. As a result, malicious actors cannot use the peripherals to listen to conversations in the area around the phone even if they gained unauthorized access to the device.

In contrast, modern softphone solutions run on multi-purpose PC’s that maintain persistent connectivity to peripherals such as microphones, speakers, and cameras, significantly expanding the potential attack surface. Since most secure areas require that built-in collaboration peripherals like these be disabled in BIOS on PC’s running collaboration softphone clients, external peripherals are required. Understanding the implications of the use of external peripherals with softphones instead of traditional desk phones is critical to maintaining the countermeasures for TSG-aligned compliance as mandated by government policy.

## 2. The Evolution of Government Telephony

Government telephony has historically been defined by tightly controlled, purpose-built hardware systems that prioritized security and reliability within well-defined physical and network boundaries. Early analog voice systems evolved into digital private branch exchange (PBX) infrastructures and later into Voice over IP (VoIP) servers with desk phones as the endpoint. Despite these technological advancements, the fundamental security model positioned telephones as stand-alone devices with limited interfaces, enabling the implementation of strong, hardware-based protections against eavesdropping and signal manipulation.

The emergence of software-based communication platforms has fundamentally altered this model by converging voice, video, messaging, and content sharing into a single collaboration application on general purpose endpoints like the PC. In this paradigm, the same device used for computing functions also becomes the primary communication platform. This convergence eliminates the clear separation that once existed between telephony systems and general computing environments, thereby expanding the system boundary. The merging of multiple communication channels onto a single platform has introduced new capabilities but still exposes the same risks that TSG-approved phones addressed in traditional telephony environments.

## 3. TSG Security Principles in a Softphone Context

Even as the industry transitions to softphones, the foundational principles of TSG guidance remain directly applicable within the broader assurance framework defined by CNSSI 5000. At the core of these principles is the requirement that communication devices must be physically incapable of transmitting audio when not actively in use. This requirement reflects a fundamental objective of national security systems for preventing unauthorized data exfiltration, including through non-traditional channels such as acoustic or peripheral-based pathways. As a result, the traditional assumptions underpinning TSG-compliant telephony must be reconsidered and re-engineered to address this broader and more dynamic threat landscape.

In legacy desk phone environments, this assurance was achieved through mechanical or electrical disconnection of microphone circuits when the handset was on-hook and the phone not in use. The user's physical interaction with the device directly controlled the state of the audio path, providing clear and deterministic assurance of non-transmission. In modern softphone environments, however, user interaction is mediated through software interfaces, while the underlying hardware remains continuously connected. Microphones, speakers, and cameras are persistently available to the system, regardless of whether a communication session is active. This decoupling of user intent from hardware state

undermines the assurance model required for systems operating under CNSSI 5000 guidance and necessitates the use of additional controls.

Additionally, modern communication platforms integrate multiple modalities, enabling seamless transitions between voice, video, and data sharing. While this capability enhances operational effectiveness, it also increases the risk of unintended information exposure. A compromised or misconfigured endpoint could potentially transmit not only audio but also visual data or sensitive content displayed on-screen. The persistent availability of microphones and cameras further amplifies this risk, as these devices may be activated without explicit user awareness or intent of the user. Within the CNSSI 5000 framework, where the protection of national security information extends across all potential exfiltration pathways, this expanded attack surface represents a critical concern.

## 4. Hardware Assurance Through Positive Disconnect Devices

To address the inherent limitations of software-based controls and restore compliance with TSG principles, it is necessary to reintroduce hardware-enforced assurance mechanisms into the communication architecture. Positive Disconnect Devices (PDDs) provide this capability by establishing a physical control point between the PC and its audio/video peripherals. These devices are designed to interrupt electrical pathways through the same physical circuitry built into TSG-compliant phones. Just as with desk phones, when communication is not actively authorized, no signal can be transmitted regardless of the state of the PC or the softphone client.

In a softphone environment, the PDD effectively serves as the functional equivalent of the handset in a traditional desk phone, reestablishing a direct relationship between user action and hardware state. When the PDD is in its secure state, microphones, speakers, and cameras are physically disconnected, eliminating the possibility of unauthorized transmission. When communication is required, the user can enable the device using a TSG button, temporarily restoring connectivity. This model provides clear, user verifiable assurance of system state and ensures that critical security controls remain effective even in the presence of software compromise.

The reliance on external peripherals in softphone architectures extends the system's trust boundary beyond the endpoint itself, requiring careful management of all connected devices. Headsets, webcams, and microphones must be treated as integral components of the communication system and subject to the same level of scrutiny as the endpoint and application layers. In secure environments, wired peripherals are mandated due to their reduced susceptibility to interception and unauthorized access.

The use of push-to-talk functionality further enhances control by ensuring that audio transmission is always an intentional user action. Webcams, when permitted, must be

governed by the same hardware-enforced controls as audio devices and may require additional safeguards to prevent unauthorized activation. All peripherals must be routed through a Positive Disconnect Device to ensure that their connectivity is physically controlled and not solely dependent on software configurations.

## 5. CONCLUSION

The transition from desk phones to softphones represents a significant evolution in government communications, enabling more efficient and effective collaboration across mission environments. However, this shift also challenges established security models rooted in TSG guidance identified by CNSSI 5000 principles. The persistent connectivity of microphones, cameras, and other peripherals within a softphone-enabled endpoint introduces risks that cannot be adequately mitigated through software controls alone.

CIS Secure was the first to introduce the Positive Disconnect Device to government agencies and supporting organizations by implementing a hardware control designed to achieve compliance with CNSSI 5000 guidance for the use of softphones in secure areas. As the leading provider of TSG-compliant desk phones, CIS Secure reintroduced the hardware-enforced control mechanism to softphones using a PDD. By leveraging a CIS Secure PDD and CIS Secure compliant peripherals, agencies can successfully deploy modern communication architectures while preserving the integrity and confidentiality of sensitive information.

Learn more about these CNSSI principles by downloading our TSG Primer white paper. See how we can help you understand your options and achieve TSG compliance!