CIS Secure TSG-Compliant Softphones Checklist

This checklist summarizes the key controls needed to deploy TSG-compliant softphones in secure areas. It guides teams through defining protected spaces and compliance requirements, selecting approved collaboration platforms and client configurations, disabling built-in peripherals, and using compliant external devices through positive disconnect controls. It also emphasizes validating the secure state through repeatable testing, publishing user guidance and training, and maintaining inventory records so deployments remain auditable and aligned with agency security policy.

Requirement	Complete (Yes/No)	Next Steps/Notes
Know your Environment - Review the environment in your Physically Protected Spaces (PPS) and where your Safeguarded/Classified Discussion Area (SCDA) lie within those spaces. Supporting Documents: Floor plans identified PPS and SCDA		
Confirm your Requirements - Work with your Department or Agency Applicable Security Authorizing Official (ASAO) responsible for maintaining an acceptable risk posture to inform you of compliance requirements for Controlled Unclassified Information (CUI), Secret, TS and higher levels of classification. Supporting Documents: Agency policy designating TSG and TEMPEST compliance for SCDA's.		
Identify your Platform - Work with your Department or Agency IT teams to identify your softphone collaboration platform. Common examples include On-Prem VoIP solutions like Cisco Jabber or Federal Risk and Authorization Management Program (FedRAMP) approved cloud solutions like Cisco Webex, Microsoft Teams and Zoom for Government. Supporting Documents: Softphone clients (maybe more than one depending on Department or Agency)		

Requirement	Complete (Yes/No)	Next Steps/Notes
Softphone Client - Establish (and keep updated) a softphone client revision level with approved client configurations for device behavior settings and logging. Artifact: Published policy and documentation for IT teams on the software side and setting baseline recommendations on the end user side.		
Disable Built-in Peripherals - TSG compliance requirements dictate that built-in microphone, speaker, and camera are disabled in BIOS/UEFI. Artifact: Validate that your IT team has disabled the on-board peripherals in BIOS.		
Deploy USB Positive Disconnect Devices (PDD) - Deploy positive disconnect devices to PC endpoints in SCDAs. All compliant softphone peripherals (microphones, speakers and cameras, if permitted) must be routed through the PDD; these peripherals may not be directly connected to the PC. Supporting Documents: connection diagram and brief connection instructions or video showing the connection process. **Headphones** - Compliant headphones can connect to the PDD and must be wired only and may not contain any radios such as Wi-Fi, bluetooth, etc. Headphones must not employ any active noise cancellation. Supporting Documents: Publish a list of compliant headsets supported by the Agency or Department.		
Push-To-Talk (PTT) - PTT devices such as headphones and handsets govern audio transmission by requiring continuous, intentional user action of pressing a button when speaking and stop immediately when released. Supporting Documents: Publish a list of compliant PTT headsets supported by the Agency or Department and the SCDAs in which they are required.		
Webcams - Compliant webcams can connect to the PDD and must be wired only and may not contain any radios such as Wi-Fi, bluetooth, etc. Webcams must also have a physical lens cover, must not have a microphone, must contain any additional ports (such as USB) and must have an active light LED visible from 360-degree perspective. Supporting Documents: Publish a list of compliant webcams supported by the Agency or Department.		

Requirement	Complete (Yes/No)	Next Steps/Notes
Execute Test Plan - Once the softphone client is configured, the PDD installed and the compliant peripherals connected, execute a battery of repeatable tests to demonstrate that in the secure state no audio/video is transmitted regardless of software state (including app running/crashed). Ensure that OS/device settings do not expose additional active microphones (e.g., monitor mic, webcam mic, docking station audio) outside the PDD path. Supporting Documents: Develop, document and archive a closed-loop testing plan where all non-conforming tests are evaluated, remediated and re-tested.		
Conduct User Training - Publish clear end user deployment and usage guidelines to ensure that end users are aware of the functionality and their obligations to maintain compliance based on Department, Agency and Government policy. Supporting Documents: Develop a User Training Guide with clear instructions and screenshots. An accompanying video is recommended.		
Inventory Management - PDDs should be inventoried and managed as tracked assets with individual serial numbers for support purposes. Supporting Documents: Asset management tracking and control system or spreadsheet.		
Conduct User Training - Publish clear end user deployment and usage guidelines to ensure that end users are aware of the functionality and their obligations to maintain compliance based on Department, Agency and Government policy. Supporting Documents: Develop a User Training Guide with clear instructions and screenshots. An accompanying video is recommended.		
Inventory Management - PDDs should be inventoried and managed as tracked assets with individual serial numbers for support purposes. Supporting Documents: Asset management tracking and control system or spreadsheet.		