JESKELL Systems, LLC | Buyer's Guide

The Next Frontier: Securing Your Conversations

Reduce Your Risk Exposure with a TSG-Approved Secure Phone

INTRODUCTION

The constant drumbeat of cybercrime stories in the news has resulted in many of us taking precautions to protect our passwords and confidential information and even taping over our laptops' video cameras to prevent unwanted prying eyes and protect one's privacy. Yet, we rarely consider that someone may be eavesdropping our conversations at work as we discuss confidential or sensitive information. This is troubling since individuals, governments and other organizations engaged in criminal or other illegal activities are transforming phones into listening devices.

IT TAKES MORE THAN A STICKY NOTE TO PROTECT CONVERSATIONS.

The U.S. has long required that federal agencies and other organizations securely protect classified data from eavesdropping and other intrusions. Recently, remote eavesdropping of unclassified communications has emerged as a vulnerability with serious consequences for governments and companies in the U.S. and around the world. CIOs, IT networking professionals, and security officers are now under pressure to protect sensitive information over the phones, AND in the vicinity of the phones.

Just consider how leaked unclassified phone conversations about criminal investigations could impact public safety or an FDA approval of a high-profile drug could enable insider trading. Leaks to the media also are threats. The Canadian government, for example, recently spent millions of dollars soundproofing the offices of Prime Minister Justin Trudeau and other meeting facilities in the House of Commons.

In the U.S., new federal mandates and security guidance, such as Controlled Unclassified Information (CUI), standardize the handling of sensitive unclassified information by federal agencies and departments. Such information may pertain to law enforcement, trade, patents, interest rates, personnel records, clinical trials, and numerous other federal activities.

One especially vulnerable entry to eavesdropping unclassified information is via phones connected to today's pervasive Voice over Internet Protocol (VoIP) networks—even when phones are on-hook or powered off. Unlike analog-based POTS service, VoIP systems operate phones on an IP based network that functions as simple computers with a microphones and network connectivity, but without the security software typically installed on workstations. Hackers can easily administer phone features remotely and listen to conversations. Further, eavesdropping voice conversations is not traceable since there is no data trail.

As a result, the National Telecommunications Security Working Group (NTSWG), formerly the Telecommunications Security Group (TSG), as part of the Committee on National Security Systems (CNSS) has issued CNSSI 5000/5001 directives to federal agencies to adopt secure phones, also known as TSG phones, to protect against audio eavesdropping from internal or external threats. If you haven't already, we recommend you join the many federal agencies that are adopting secure phones for unclassified communications before your organization's conversations thought to be private are inadvertently breached.

WHERE AND WHAT TYPE OF SECURE PHONES DO WE NEED?

The first step is to establish if secure phones are needed in your environment to protect information or comply with the new federal mandates for unclassified communications. If the answer is yes, then you need to determine where and what type of secure phones your organization needs.

There are two levels of protection. Class A provides additional security for secure phones connected to a switch installed in an area with a lower protection level than where the phone is located. Class B secures phones connected to switches installed in areas with the same or better protection levels as the phones' location.

Class B phones protect the speakerphone and handset from remote activation, prevent network cables from transmitting audio when not in use, secure headset ports, and provide other security capabilities. Slightly more expensive Class A phones include all these security features, as well as power injectors used to defeat internal threats exploiting Power over Ethernet (PoE). Class A and Class B TSG phones are different from TEMPEST phones, which protect against leaking electronic emanations.

REDUCE YOUR RISK EXPOSURE WITH A TSG-APPROVED SECURE PHONE

At Jeskell, we offer a TSG-approved secure phone solution via the NITAAC CIO-CS government-wide acquisition vehicle. Designated by the Office of Management and Budget (OMB) as a best-in-class contract, the CIO-CS vehicle greatly simplifies procurement of IT products, services, and solutions by any federal civilian or Department of Defense agency.

Jeskell is a full-service systems integrator with more than 25 years of experience serving the federal government and is a participant in National Industrial Security Program. Our staff, many of whom maintain top-secret security clearances, offer deep, proven technical competencies and understanding of federal regulations and requirements.

Often, maintaining legacy IT infrastructure environments slow adoption of more innovative and cost-effective technologies. We collaborate closely with our customers to overcome the complexity of these challenges while enabling fast, cost-efficient deployment. Using our in-depth IT technical and security expertise, we're able to help you select and implement a secure phone solution that is compliant with federal IT and telecommunications security mandates and interoperable with your existing infrastructure.

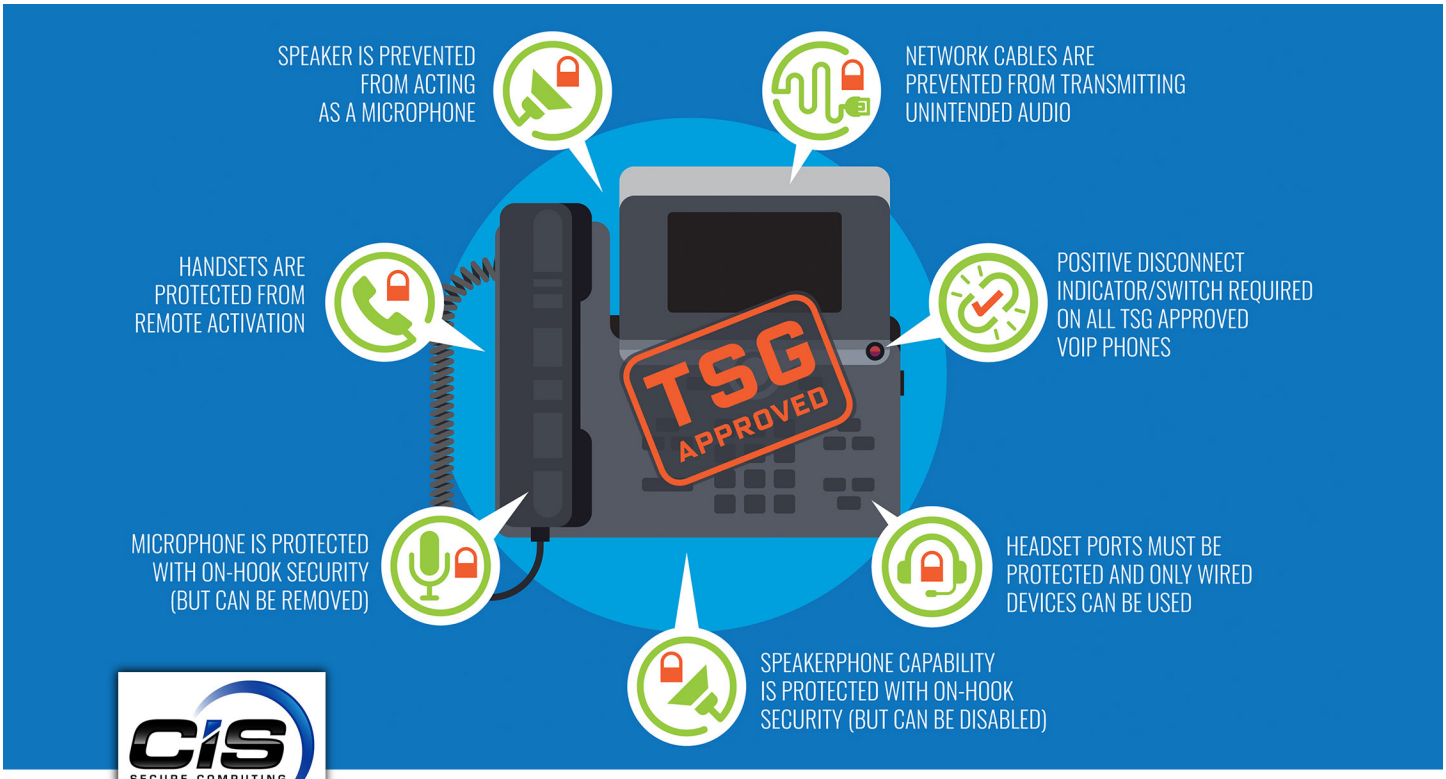
AN OFFICE PHONE CAN BE A LISTENING DEVICE EVEN WHEN NOT IN USE.

Our partner, CIS Secure Computing, the worldwide market leader for TSG-approved VoIP instruments and devices, modifies and delivers phones supplied by Cisco, Avaya and Polycom as part of Jeskell phone solution packs. These phones provide government certified on-hook security for all unclassified VoIP telephony systems installed in U.S. government or U.S. government contractor spaces where national security systems are employed or where classified national security information is communicated, processed or stored. CIS devices also may be compliant with CUI in accordance with the federal organization's risk requirements. Such CUI may include For Official Use Only (FOUO), Law Enforcement Sensitive (LES), and Sensitive but Unclassified (SBU).

We offer standard bundles of 10, 25, 50 and 100 secure Cisco, Avaya, or Polycom phones with options for Class A or Class B levels of protection, as well as additional options for customization.

Here are some of the capabilities of our TSG-approved secure phone solution packs:

- Push-to-talk restrictions, disabled speakerphones, removed microphones, among other options
- Approved for use in SCIF and SAPF environments
- On-hook security features providing enhanced Hold and Mute security during calls and protection of speakerphone and headset ports
- Compatibility with wired headsets but not approved for wireless headsets
- USB positive disconnect for headsets, soft phones, and web cameras (i.e., Jabber, Skype, and Scopia) that includes an integrated time out feature with discreet logic that cannot be programmed or reprogrammed
- Remote disabling of speakerphone available via telecommunication provider control application manager (e.g. Cisco Unified Communications Manager, Aura Call Control)



TSG PRODUCTS FROM CIS SECURE COMPUTING ARE MADE IN THE USA.

ENSURE SUCCESS WITH ENHANCED DEPLOYMENT AND TRAINING SERVICES

For all our secure phone solutions, we will work with you to understand your security requirements, unclassified environments, and telecommunications infrastructure. Jeskell also will collaborate with you to determine and implement the best secure phone solution according to your budget and requirements and any needed customization.

For customers that desire assistance with deployment and training beyond the basic quick start services, we offer a range of enhanced implementation options that can be bundled with the phone solution pack for an additional cost. Here are several of the enhanced services available to our secure phone solution customers:

- Enhanced training and testing
- De-skidding, unboxing and removal of all packing materials
- Removal, safe and proper disposal, and treatment of old equipment
- Possible trade-in of old equipment
- Cabling and wiring
- Custom colored faceplates
- Powering and configuration of new secure phone on existing network, using existing cabling, or connecting new GFE cabling from existing wall jack to desk switch and/or secure phone
- Device asset tagging and special marking

Our tight-knit group of IT and security experts at Jeskell will collaborate with you closely to ensure your secure phone solution is deployed successfully and protects your organizations from eavesdropping and other threats that may compromise your agency's mission. Your success is our success and that will be evident every step of the way from initial planning to post-integration support.

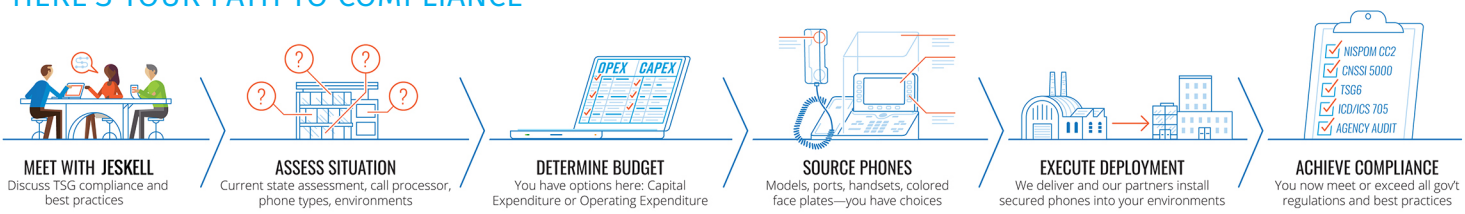
AN EXPANDING FRONTIER FOR SECURE PHONES

As agencies and legislative offices move quickly to secure VoIP phones, financial services, healthcare, legal and other environments engaged in sharing of unclassified sensitive information soon will be implementing secure phones as well.

The U.S. government is already preparing mandates for federal agencies to secure mobile phones connected to both WiFi and cellular networks. For now, we recommend federal organizations provide staff with guidelines on the type of information that can be discussed on mobile phones and choose mobile phones with extensive security features.

Meanwhile, we hope you will contact us to help you evaluate your current exposure to eavesdropping and other threats that could seriously compromise your information. We are confident that we will recommend solutions that help your organization successfully deliver on your mission and objectives as securely, efficiently, and quickly as possible.

HERE'S YOUR PATH TO COMPLIANCE



Want to talk to the expert? Contact:

Tony Celeste

Vice President, Strategic Initiatives

Office: (301) 230-1533 ext. 917

Mobile: (301) 602-2353

Email: tceleste@jeskell.com

To learn more about how Jeskell can help your agency achieve its vision for IT modernization and security, visit us online.