ribbon®

Finding the right voice
Where do federal agencies stand in adopting greater cloud voice solutions?

eBook

In this eBook, we will look at the trade offs of cloud flexibility, premises resiliency, and end to end security in a new collaborative world of communications.

Getting to the cloud—or getting to the right cloud—for voice solutions has often been a slow grind for U.S. federal agencies, personnel and partners trying to equip themselves with the best, safest and most economical networks for reliable and resilient voice solutions. For many IT decision-makers at those departments, it's not a simple answer.

Change is good: the pandemic made change an imperative

Prior to COVID-19, moving to a cloud-based voice system was a distant "someday" proposition based upon lack of contemporary cost-effective options and the comfort—even the luxury—of having the local office supported by a secure and reliable PBX system built to federal requirements.

Post-pandemic though, that "someday" is today. Premises-based voice systems became expensive dead assets during the pandemic, mostly or entirely unusable by teleworking employees. Some federal agency personnel were able to cope during lock-downs with teleconferencing and cell phones, but these solutions were not applicable to employees who needed secure federal communications that they could, unfortunately, not enjoy. Temporary measures were taken, but those measures were stopgap and could not sustain long-term, secure voice communications accessible from any location.

An unintended byproduct of long-term teleworking is the growth in implementation of collaboration tools like Microsoft Teams and Cisco Webex. Prior to the pandemic, most federal collaboration consisted of face-to-face meetings and/or call-in conferencing for employees traveling or working from home one-to-two days a week. But extended teleworking has made it apparent to federal agencies that their team members can accomplish much of the same levels of collaboration and work efficiency through the use of easy-to-access voice, video, messaging and file sharing capabilities, regardless of the physical location of those employees.
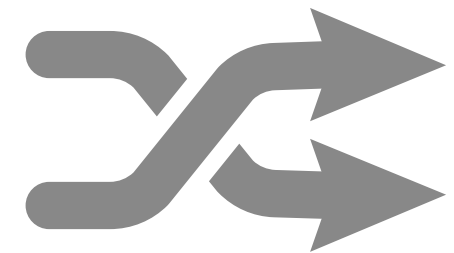
The human touch

Many [studies](#) have shown that in communications with other people, visual cues convey the most information, followed by the sound of one's voice. Interestingly, the actual content of the communication conveyed the least amount of information. The most successful collaboration tools acknowledge that with their easy-to-use video conferencing and add on workplace efficiency tools that increase productivity, like consolidated messaging, easy to manage team environments, file sharing and other functions.

Those sensory factors contributed to the massive growth in implementation of collaboration tools during the pandemic. Zoom was a leader in this space, owing to its ease of use and free trial usage, mushrooming from 10M daily active meeting participants in December 2019 to 300M by April 2020. Microsoft Teams, more focused on enterprise usage, reported 20M licenses users in November 2019 and 115M licensed users in November 2020.

Will these tools continue to see widespread federal agency use post COVID-19? The clear answer is yes–most agencies have seen a significant demand by their personnel to allow continued usage after a return to "normal" operations. While many agencies are planning on continuing the use of expanded teleworking, eventually a large number of federal personnel will return to some modicum of on-site office work. But the value of collaboration tools remains undeniable–even in an office environment. The combination of voice, video, messaging–combined with other corporate IT tools–reduces the need for travel and even in-person meetings. For large agencies with offices or bases throughout the continental United States or even outside its perimeters, the power of these tools to increase mission effectiveness and efficiency has been realized. by nearly every federal agency.

The human touch

The added benefit, and by a significant margin, of the adoption of these advanced collaboration tools is their cloud availability and resiliency. The tools can be accessed anywhere, and teleworking federal employees can have the same access to communication and collaboration tools as any office worker.

Many private enterprises have moved to significantly expanded–even to permanent–telework. Productivity has not suffered, according to most economists, for many companies or employees during government-mandated quarantine orders. In some cases, there has even been an uptick in productivity due to reduced commuting time and increased family time. And with that, many companies are looking to the future, questioning the value of expensive real estate and the potential expenditures in business travel post COVID-19.

Federal agencies don't have the same personnel management flexibility as corporations, so complete teleworking–or significantly increased teleworking after the pandemic is over–may not be an option for most agencies. But the power of cloud-based collaboration will not diminish and the federal government will have new options for flexible work environments to attract and retain talent, as well as new ways to use collaboration tools as a larger mission-enabler.
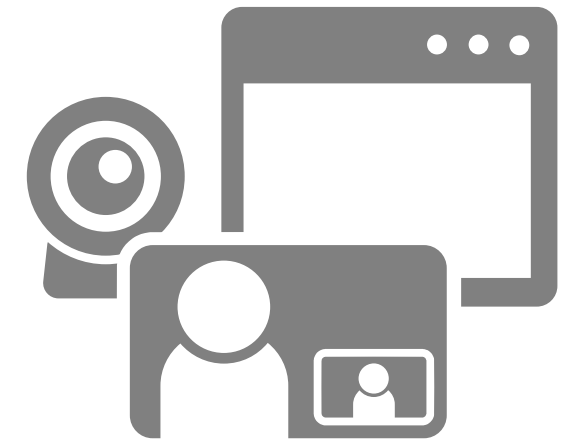
Importance of voice solutions in a federal setting

Collaboration tools like Microsoft Teams and Zoom are not a replacement for a phone systems. And voice capabilities remain a requirement for nearly every federal agency. Similar to plumbing, the ability to pick up a phone and call the right person or persons, securely and reliably, regardless of what emergency the agency or country is facing will always be important. While collaboration tools are powerful and resilient, and while they do replace many functions of a phone system, they are not a replacement for secure and guaranteed voice connectivity. At the same time, voice solutions are expensive–and they cannot and should not break the bank for any agency.

So, the key question for federal agencies: how can the agency move forward to cloud-based voice solutions, preserving existing capabilities still required of their premises-based phone systems, but start to migrate to cloud capabilities as it makes sense?

Ribbon advocates sensible and practical approaches that are sensible and fit within the agency's needs and budget. Those solutions will support the federal agency journey toward full cloud voice adoption that retains the security, resiliency and flexibility of their already-existing premises voice requirements. And the agency must find a pace that make sense for its budget, personnel needs, and state of current voice IT infrastructure.
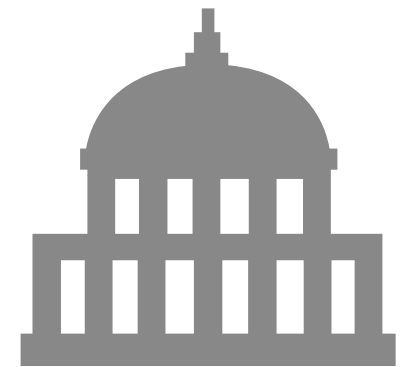
Section I: Session Border Controllers/Direct Routing

How does an agency securely and reliably connect collaboration tools to public phone networks?

How does an agency securely and reliably connect collaboration tools to public phone networks?

While collaboration tools like Microsoft Teams carry with them sophisticated communication technologies, they tend to be self-contained. Communications between users on the same cloud platform tend to be very easy to initiate and terminate because they are on the same network. When it comes to connectivity to the PSTN however, it is a little more complicated. PSTN providers (Verizon, AT&T, Lumen, etc.) operate with standard communication protocols for voice, like the public Internet for data communications. With Internet connectivity, a federal agency cannot and will not connect its systems to the public Internet without security protections, such as firewalls and gateways. In voice connectivity, that protection is a Session Border Controller (SBC).

Enterprise session border controllers (SBCs) are situated at the edge of the enterprise network and provide secure voice and video connectivity to Session Initiation Protocol (SIP) trunking providers, users in remote branch offices, home workers/remote workers and unified communications as a service (UCaaS) providers. The name "session border controller" is derived from the session, from Session Initiation Protocol, referring to a real-time communication connection between endpoints or users. This is typically a voice and/or video call. Border refers to the interface between networks that do not have full trust of each other. Controller refers to the ability of the E-SBC to control (allow, deny, transform, end) each session that traverses the border.

So where should SBC's be placed to support cloud collaboration tools? Well, the answer is, of course, "it depends."

How does an agency securely and reliably connect collaboration tools to public phone networks?

If an agency was going to go solely cloud-based in its communications, then it likely makes the most sense to have a cloud-based SBC. A cloud-based SBC can be hosted and managed in a federally compliant cloud environment, such as Microsoft Azure, Amazon Web Services or other FedRAMP compliant cloud hosting services. At that point, voice circuit connectivity between the cloud the SBC is hosted in and MS Teams can be established. For agencies still requiring some level of premises-based voice support, it may be cheaper and faster to put the SBC within their own offices. As another option, several vendors offer SBC as a service from among their FedRAMP compliant cloud offerings.

A premises-based SBC can be less expensive than a hosted SBC since hosting charges for the SBC hardware/software don't apply. In addition, some SBC vendors, such as Ribbon Communications, offer their SBC products as a subscription, instead of an upfront capital purchase. In these scenarios, additional voice circuit costs may apply to the agency to connect the SBC to the MS Teams cloud offering. In addition, the agency would also be responsible for the SBC maintenance, upgrades and support.
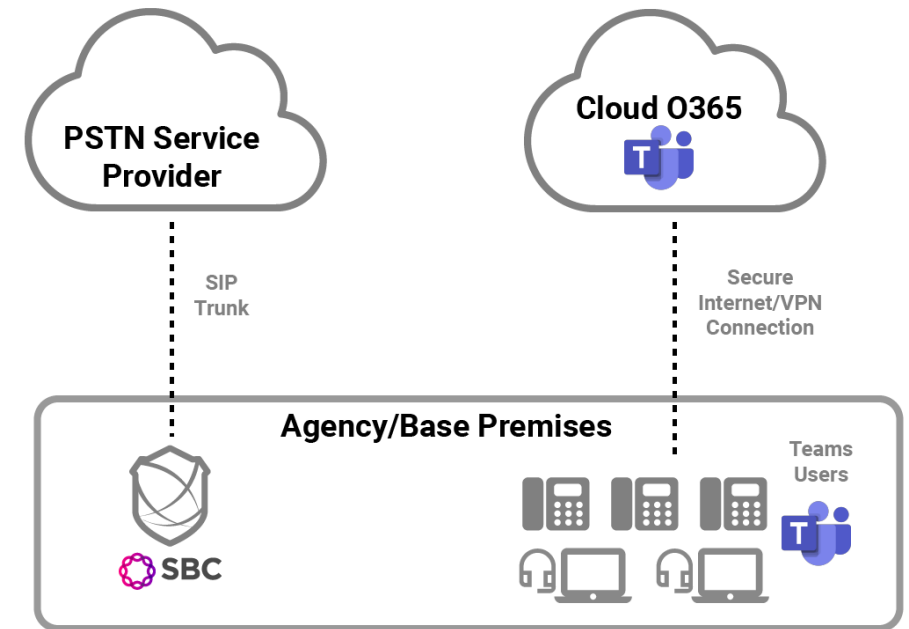
Diagram 1: SBC on Premises

How does an agency securely and reliably connect collaboration tools to public phone networks?

A hosted SBC is typically purchased on a subscription basis versus an upfront purchase, so over time it may end up more costly to the agency. However, it can be easier to procure hosted SBC services as a monthly or annual cost versus the internal cost justification for a capital acquisition purchase request. In addition, depending on what hosted service the agency chooses to host their SBC in voice circuit, connectivity to MS Teams may already be established. The agency would still be responsible for the SBC maintenance, upgrades and support, however.

Lastly, there are several offers for Federal FedRAMP and JITC approved SBC's as a service to enable Direct Routing in which the Cloud Service Provider will own and operate the SBC on the agencies' behalf. While these offers tend to be more expensive, they have the benefit to the agency to be a true one stop shop, offering the SBC capability, voice circuit connectivity, and overall management of the service so the agency only has to work with a single vendor for this capability.
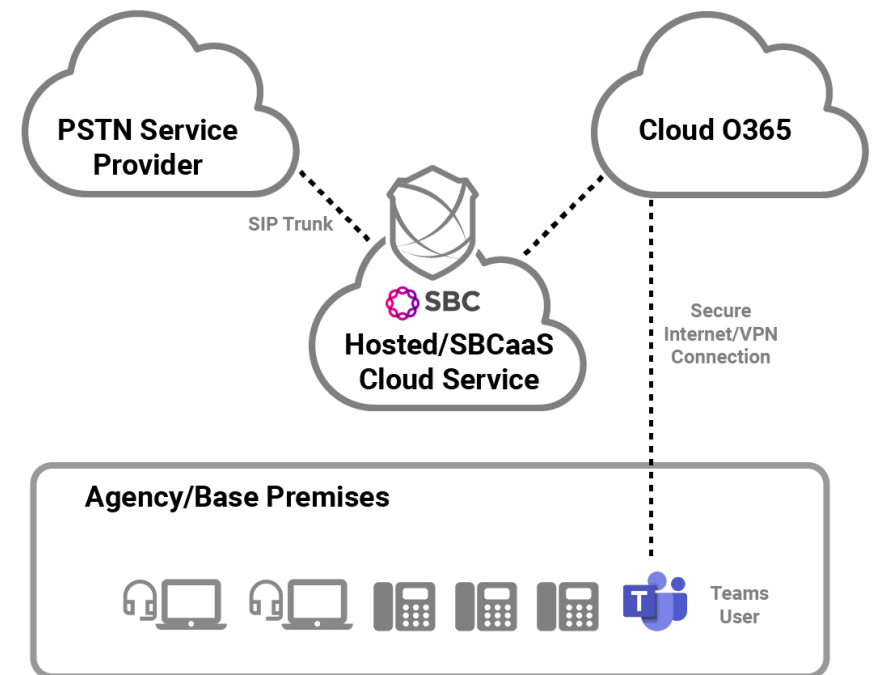
PSTN Service Provider

Cloud O365

SIP Trunk

SBC

Hosted/SBCaaS Cloud Service

Secure Internet/VPN Connection

Agency/Base Premises

Teams User

Diagram 2: Hosted SBC/SBCaaS

How does an agency securely and reliably connect collaboration tools to public phone networks?

Table 1: Premises SBC/Direct Routing

| Benefits	Things to consider
Ease of deployment	Additional cost for voice circuits to premises
More control over solution by having it local to IT environment	Additional resources to manage premises voice environment
Potentially lower total cost of ownership structure	Backup/High Availability architecture to insure uninterrupted operation

Table 2: Hosted SBC/Direct Routing

Benefits	Things to consider
Ease of deployment	Potentially higher cost structure
Administration/upgrades/maintenance handled by clouds service provider	Cloud Service Provider uptime guarantees and Service Level Agreements (SLA)
Potential reduction in resources to manage voice environment	Portability of service to competing providers
Flexible usage and cost–not tied to fixed premises environment	
Aids in disaster recovery	

Section II: What about premises devices and local survivable hosted collaboration tools?

What about premises devices and local survivable hosted collaboration tools?

While most of the recent popularity of collaboration tools has focused on teleworking flexibility and new ways of employee engagement and collaboration, a stark truth exists: many federal agencies have many premises analog devices that cannot be easily migrated to SIP. These include hallway phones, common area phones, guard shack phones, and many other examples. The cost of SIP migration can be very high for the devices themselves because of the wiring and cable plant issues required to migrate these devices to SIP. These analog devices, though, are still critical to mission-critical operations, and cannot be forgotten in any agency voice strategy.

Some federal agency IT organizations have come to the conclusion that leaving analog ports on the old PBX system is less expensive than incorporating them into a UC rollout. This problem has driven many enterprises to keep their legacy PBX systems in service for years beyond the original schedule in order to defer this cost. Unfortunately, this option gets more expensive each year as maintenance costs for aging equipment are constantly increasing, and experienced PBX engineers are getting harder to find and to keep.
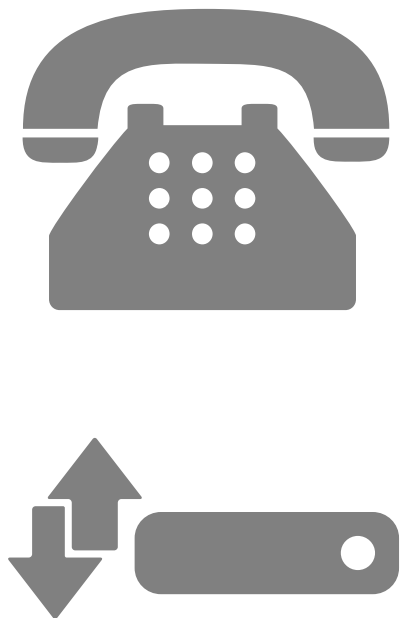
What about premises devices and local survivable hosted collaboration tools?

In the move to cloud-based collaboration tools, agencies are likely unable to bear the cost of both an aging premises-based PBX as well as the collaboration tools that the user demands. As a result, many agencies are forced to choose between supporting legacy endpoints.

In this case, the solution is a local analog gateway. An analog gateway, consisting of dozens or even hundreds of analog ports, can be deployed at an agency headquarters, base or campus, connecting all of its various analog devices. The gateway is then connected to an SBC to allow calls to be placed to the PSTN, to 911, or to cloud based users in a cloud collaboration tool. In the event of a communications interruption to a cloud-based collaboration solution– such as a cloud outage, a weather emergency, or a security incident–the analog gateway can insure uninterrupted communication with the outside world. Many gateways offer additional functionality, such as wireless or satellite backup, for redundant communications in the event of emergency.
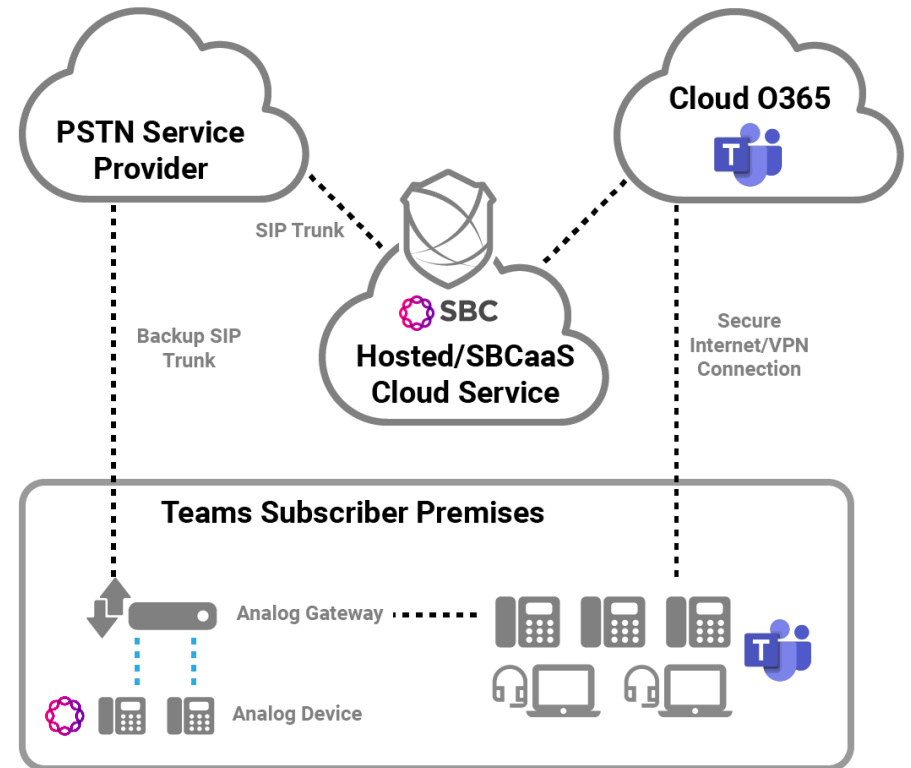
Diagram 3: Local Analog Gateway

What about premises devices and local survivable hosted collaboration tools?

In addition, as a large number of agencies move to cloud collaboration tools for a majority of their voice communications, redundant options for local collaboration usage become necessary. For example, if federal employees are accustomed to using cloud-based MS Teams as their primary communication tools, they can't afford to stop communications if there is a temporary or extended outage . The Teams Survivable Branch Appliance (SBA) gives organizations a back-up plan for phone calls if Microsoft 365 becomes unavailable for any reason.

Table 3: Local Gateway/Survivable Branch Appliance

Benefits	Things to consider
Continued local communications in the event of a cloud communications interruption	Additional cost and management of local IT infrastructure
Possible elimination of premises-based PBX infrastructure	High availability architecture to insure uninterrupted service for local disruptions (hardware failures, operator errors, etc.)
Support for legacy environment components that are too costly to replace	
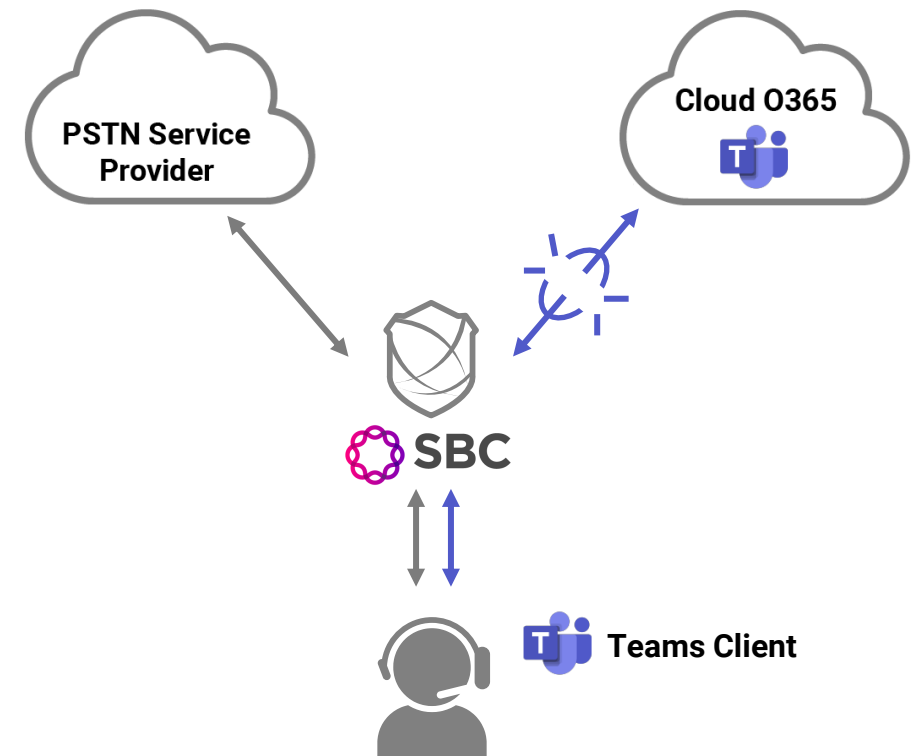
Diagram 4: Microsoft Teams Survivable Branch Appliance

Section III: Moving your agency voice systems to the cloud in a sensible, cost-effective manner

Moving your agency voice systems to the cloud in a sensible, cost-effective manner

While cloud collaboration tools are getting all of the industry press, there are still many situations that agencies face where cloud collaboration tools either don't apply or aren't the most cost-effective way to provide services to their customers.

Cloud collaboration tools enable great workplace efficiency, but they are not a complete phone system replacement. We have shown in Section I that connecting these tools to the PSTN requires the use of a Session Border Controller for connectivity and security, and these SBC's can be deployed either on the premises or in the cloud. In a similar fashion, connectivity to products and tools that are not provided as part of a cloud collaboration solution offering can require the use of a voice solution for interworking and integration. These products and tools can include:

- E911 and next-gen 911 services
- Large-scale conferencing solutions
- Call center applications
- Alarm systems
- Video conferencing systems

In traditional voice deployments, a premises-based PBX would be the integration point for all of these types of products and tools. With cloud collaboration tools providing many of the functions of a PBX, investing in a PBX platform does not make much economic sense for a federal agency that has decided to move their voice communications to the cloud. Also, as employees gain a comfort level using cloud collaboration solutions as their primary communication tool, it makes sense to have cloud voice services, or voice-as-a-service, that augment cloud collaboration tools. These tools serve the flexible work environments that agencies are looking to adopt post COVID-19.

Moving your agency voice systems to the cloud in a sensible, cost-effective manner

Voice-as-a-service is not a new concept, but it has taken on new relevance as cloud-based collaboration tools have grown rapidly with the ascendance of remote working strategies in response to the COVID-19 pandemic. Cloud-based voice-as-a-service offerings complement cloud-based collaboration tools, allowing interworking with public telephone networks and third-party applications with all the benefits of cloud deployments: flexible usage options, voice managed services options, and pay as you go pricing.

Ribbon voice-as-a-service solutions have been architected, from the beginning, to be deployed in a cloud environment. Cloud voice services must be secure and resilient—security being an underpinning of Ribbon's technological advantage. Ribbon voice solutions were initially built to serve the needs of voice carriers, who demand secure, mission critical solutions that can scale to a very large environment as needed.

In addition, Ribbon's voice solutions are designed to support multi-tenancy. Multi-tenancy is the ability for logical, not physical, separation of user, security and administrative data while sharing computational resources such as memory, processing power, and connectivity. Ribbon multi-tenancy capabilities significantly lower the cost of voice-as-a-service, a critical factor as discerning federal agencies choose the most cost-effective and secure path to the cloud. Each new tenant on the Ribbon platform is configured so that no other tenant on the system has any ability to access or affect the new tenant's data or configuration. Competitive solutions that do not offer multi-tenancy require a physically separate instance of each voice product for every customer, with the same cost structure of deploying the voice service on an agency premises. Ribbon multi-tenancy is the key to secure, flexible and cost-effective cloud voice deployments.

Voice-as-a-Service in a public cloud

Voice-as-a-service in a public cloud is a huge economic growth area in the commercial enterprise market, spurring some companies that offer cloud voice services to grow by triple digits during the pandemic. Many of these cloud voice service offerings are already integrated to cloud collaboration offerings and other cloud offerings, such as call center and conferencing applications. So commercial enterprises can pick and choose the service offerings and levels of service that best fit their business goals.

For federal agencies, this move to cloud voice services has been a bit slower. Part of the challenge has been the much more stringent security requirements for federal public cloud offerings, known as FedRAMP. This adds cost and complexity to vendors offering cloud services, so many vendors with successful commercial offerings choose to avoid entering the federal market since they perceive it to be less profitable for them. For cloud-based voice services in particular this has been a challenge in that voice services tend to be perceived as equivalent to a utility–buyers want it cheap and users want it reliable. This has created a bit of a "chicken and the egg" problem in that with few vendors offering cloud-based voice services, there has been little demand by the federal government to issue solicitations for these services, which further fuels the perception by the vendor community that the demand is not there.

The COVID-19 pandemic has changed that dynamic, and many federal agencies are now requiring voice as a cloud service. With more of their employees teleworking and using cloud- based collaboration tools, agency IT departments are seeing a need for a more flexible, secure voice service to complement these collaboration tools. Cloud based voice services make much more sense for their IT environment versus an expensive PBX on site that does not support the new work environment.

Voice-as-a-Service in a public cloud

A public cloud based voice service that is offered by a cloud service provider can sit in FedRAMP certified public cloud voice environments just like any other application, such as e-mail. Unlike e-mail however, voice services in the cloud have a much higher requirement for low latency. Latency is delay in the network, and too much latency can provide for stuttering or delayed voice response, resulting in user frustration and complaints.

Voice service is typically delivered over public internet or private networks that are tunneled through the public internet using a Virtual Private Network (VPN) capability, or over dedicated MPLS (Multiprotocol Label Switching) circuits. Architecting the connectivity to the cloud voice environment is key to making sure that the proper prioritization is given to voice network traffic to ensure a consistent, user friendly voice environment.

This solution will ideally be deployed in the form of multiple node deployment of Enterprise / Core Session Controllers that can seamlessly accommodate the automatic redeployment of users without provisioning or heavy administrative operation. This will provide for a highly fault tolerant call control fabric, minimizing exposure to maintenance windows, outages, and denial of service attacks, and it will serve as a mechanism to manage the core solution as an "always on" infrastructure. The placement of an Enterprise Session Controller in a hardened public cloud will enable secure voice communication services to users, as allowed by security guidelines. Remote workers can access voice services from this cloud, and network routing can be configured to route calls to and from users registered to this system to simultaneously be delivered to other destinations on the network, such as a local session controller located on a customer premises or to Microsoft Teams.

Voice-as-a-Service in a public cloud

The core solution can integrate with collaboration platforms such as Microsoft Teams in several ways. Many collaboration solutions support Direct Routing of calls into the collaboration environment, where users can place or take calls within the collaboration user experience. This integration, coupled with routing logic in the core voice solution will provide the ability for users to originate voice calls within the collaboration client without forcing the user to use another client to place voice calls.

Voice-as-a-service in a public cloud is a cost effective and secure option for federal agencies looking to modernize their voice environment as they look toward more flexible offerings post-pandemic. There are several FedRAMP moderate and FedRAMP high offerings currently available by vendors using Ribbon technology.
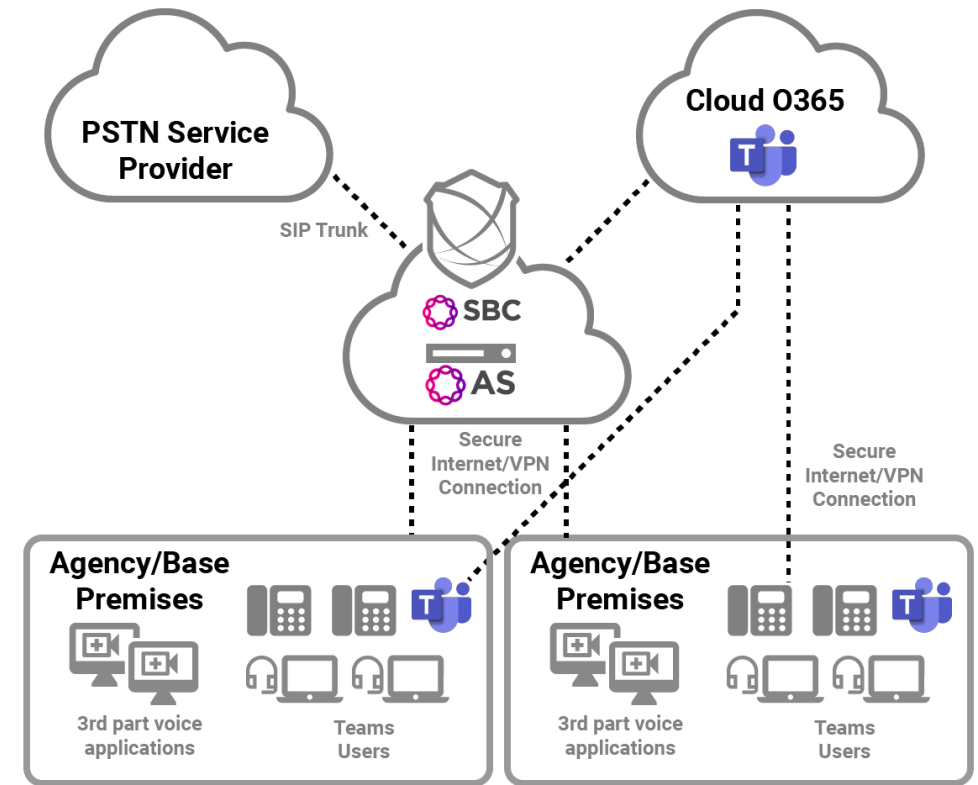

Diagram 5: Public Cloud

Voice-as-a-Service in a private cloud

While a public voice-as-a-service option may work for some agencies, larger agencies, or agencies that require a higher level of customization and control over their voice environment, may look to deploy a voice service in their own private Federal cloud. This approach enables greater control of management and security for the solution, while carrying many of the same benefits as a public cloud approach. This "core solution" – a Session Controller in the FedRAMP Moderate or FedRAMP private cloud -- can be used to replace the aging soft switch network, providing greater control of call distribution among public cloud and on-premises infrastructure.

A private cloud can be defined as moving the PBX into a cloud-based data center instead of a locally operated data center, easing the transition of voice services to the cloud while still retaining control over the voice environment. While costs may be higher because of the lack of economies of scale inherent in the offering being built for just one customer versus many, larger agencies may find that having the flexibility and control, along with the ease of administration of a multi-tenant environment, to be worth the higher cost.
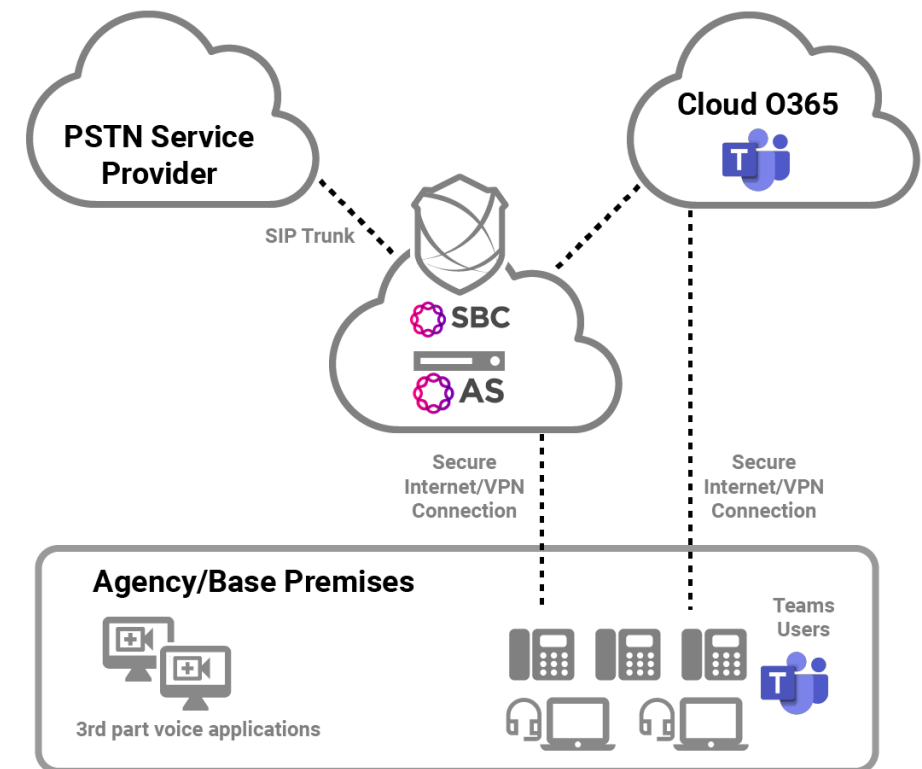
Diagram 6: Private Cloud

Voice-as-a-Service in a private cloud

Table 4: Public Voice-as-a-Service Cloud

Benefits	Things to consider
Potentially lower cost through reduction/elimination of premises voice environment	Less customization of voice environment
Cloud availability	Potential risk of cloud communication failure or service interruption
FedRAMP security controls	Cloud Service Provider uptime guarantees and Service Level Agreements (SLA)
Administration/upgrades/maintenance handled by clouds service provider	Portability of service to competing providers
Flexible usage and cost versus upfront capital cost	

**Table 5: Private Voice-as-a-Service Cloud**

Benefits	Things to consider
Potentially lower cost through reduction/elimination of premises voice environment	Potential risk of cloud communication failure or service interruption
Cloud availability	Cloud Service Provider uptime guarantees and Service Level Agreements (SLA)
More control over voice environment	Portability of service to competing providers

Section IV: Supporting your premises voice environment with hybrid cloud technologies to mitigate mission risk

Supporting your premises voice environment with hybrid cloud technologies to mitigate mission risk

For many agencies, a combination of cloud-based collaboration-tools, cloud-based voice services, and survivable local gateways will be the ideal end state for a secure, flexible voice strategy that supports a combination of office work and telework. For some agencies, particularly those who have a number of personnel involved in public safety, law enforcement, or deployed at military bases, local survivability in the event of short-term outages may not be enough. Larger offices and bases have to be prepared to operate normally in the event of potential long-term communication interruption to the cloud, and a local survivable communication tool may not be enough for days or weeks of extended periods of limited or no cloud connectivity. For these scenarios the ideal end-state for their voice infrastructure is a combination of cloud-based technologies to support collaboration and teleworking, integrated with the right amount of premises capability to support legacy technology and provide resilient operations in the event of an extended cloud outage. This is a hybrid cloud environment and is contingent upon an architecture and pricing that allows for resilient, secure, simplified, and cost-effective voice usage.
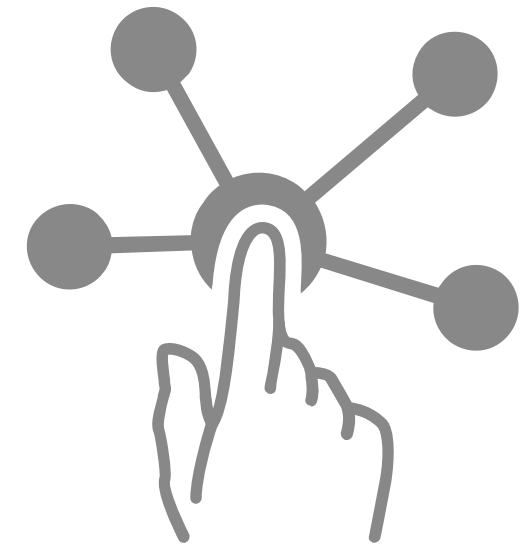
Hybrid cloud approach

A hybrid cloud approach can be engineered to meet the needs of remote work through the use of integration technologies to intelligently send calls to their destinations regardless of whether the user is accessing their voice service capabilities in the cloud or on premises. This approach enables the government to leverage public and private cloud platforms in concert with on-premises platforms to meet the needs of specific use cases.

The cloud and premises approaches represent a different prioritization of remote work capabilities versus on-premises and local control and customization, whereas the hybrid cloud approach equally prioritizes these attributes. The pure cloud approach may not be the most diverse. It leverages a cloud remote work solution for a significant portion of the user population, increasing the susceptibility of communications to be compromised during a malicious attack. The premises approach requires either remote network access over VPN for remote work, or a reduced feature set via OTT services. Notably, closing the gaps of the cloud approach brings it closer to a hybrid approach, and closing the gaps of the premises solution brings it closer to a hybrid approach.

The hybrid cloud approach will enable users to access the same set of communications services from different fixed or mobile devices, and to derive that service anywhere–across multiple networks and platforms. This approach leverages voice add-on capabilities of numerous collaboration service providers, allowing users to consume the service from within the user experience of collaboration and productivity applications.
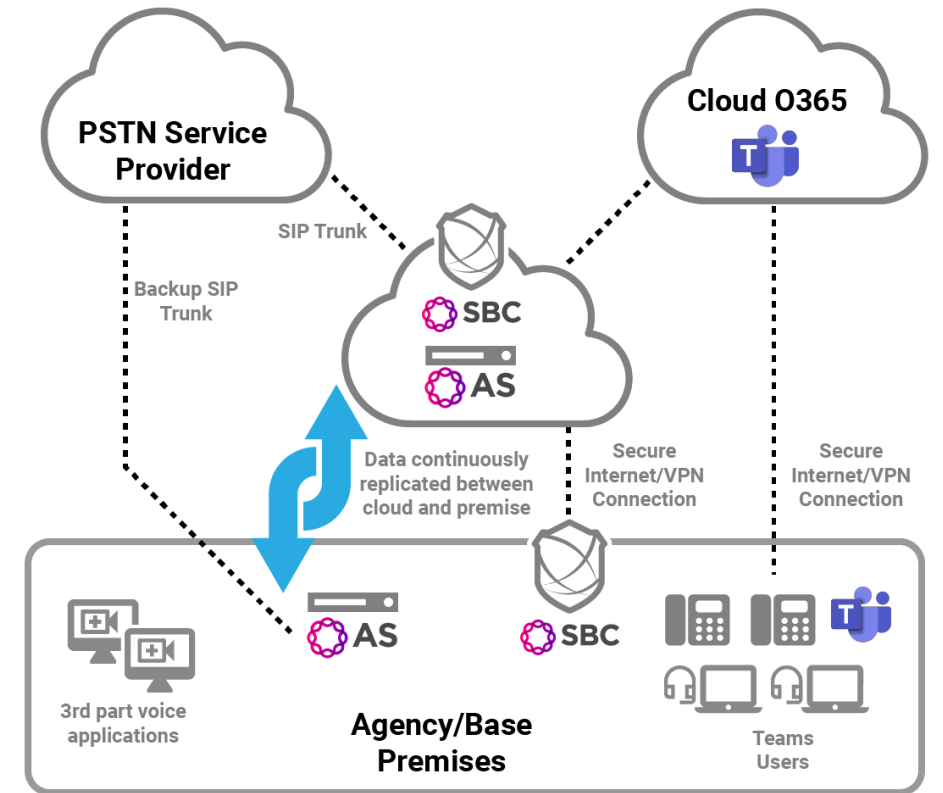

Diagram 7: Hybrid Cloud

Hybrid cloud approach

The overall solution consists of placing the voice communications infrastructure in a private cloud or public cloud environment that is hardened with FedRAMP Moderate or FedRAMP High security controls. This infrastructure serves as the core of the solution and will be integrated with the direct routing feature of Microsoft Teams and other collaboration platforms to provide for a Unified Communications as a Service (UCaaS) that is cloud based and can be accessed directly over the network or via the user experience of the Microsoft Teams or another collaboration client. This cloud-based infrastructure is then integrated with Local Session Controller (LSC) SIP PBX systems located on premises using SIP Trunks and on-premises gateways to analog devices.

A key requirement of the core UCaaS infrastructure is the ability of the UCaaS infrastructure to fork and simultaneously deliver calls across (1) devices and soft clients that are directly registered to the service,to the (2) SIP PBX systems and to (3) Microsoft Teams and other collaboration services using direct routing capabilities. Another key requirement of this infrastructure is the ability of the on-premises SBC to monitor the state of the UCaaS ESC and be capable of re-routing calls and device registrations to different CSC / ESC and LSC registrars based upon that state. A third key requirement of this infrastructure is for the Core Session Controller to operate in a "cloud native" manner in which users and SIP trunk terminations can be distributed, re-homed, or re-groomed to register to any node in the core in an automatic fashion with little or no administrative provisioning required.

Hybrid cloud approach

These key attributes allow the solution to provide their unique voice service, including assured services, in a consistent manner irrespective of the actual platform that users are registered to, or of the applications or devices that they are using.

The hybrid cloud approach meets the needs of larger agencies and bases by balancing the needs of remote workers against the needs of continuity and security for mission critical communications across defense and executive functions and organizations.

Table 6: Hybrid Cloud

Benefits	Things to consider
Both Fixed and Remote Work capability	Potential risk of cloud communication failure or service interruption
Continuity of service across networks	Cloud Service Provider uptime guarantees and Service Level Agreements (SLA)
Simplified Administration	Portability of service to competing providers
Seamless user transition to remote work	Seamless operation between on-premises and remote users
Availability of services on multiple device types	Compliance with security frameworks and hardening measures across devices and networks

Section V: Why Ribbon is the right choice

Why Ribbon is the right choice

In today's rapidly changing federal telecommunications landscape, delivering lower-cost, high-quality collaboration environments, operating networks efficiently, ensuring network security and innovating new products and services to a more discerning user are critical to success. With its myriad solutions for performance and security, Ribbon can take you there, with the premises that:

- There's a lot of grey area in federal agency decision-making about cloud voice solutions, and that's OK. Decisions don't have to be black and white. Or all or nothing. And the pandemic has changed the collaborative landscape for all sectors, including federal agencies.
- Flexible, adaptive and secure voice environments are the future of agency voice and collaboration solutions
- Premises, cloud and hybrid solutions all have their strengths and weakness to meet the agency's specific needs.

Ribbon is the industry leader in integrated premises, cloud and hybrid voice solutions, built to support collaborative communications environments in a manner that is substantially more cost-effective, secure and flexible than its competitors. Ribbon may be a new name to many Federal agencies, but we have deep roots in delivering secure, critical and innovative communication capabilities to the US government, enhancing collaboration and ensuring mission success.

About Ribbon

Ribbon Communications (Nasdaq: RBBN) delivers global communications software and packet and optical network solutions to service providers, enterprises and critical infrastructure sectors. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge IP solutions, cloud-native offers, leading-edge software security and analytics tools, as well as 5G-ready packet and optical networking solutions acquired via our recent merger with ECI Telecom. To learn more about Ribbon visit rbbn.com.