Collaborating in a Remote Environment

Rise in Remote Work

More Federal agencies have implemented work-from-home policies than ever before, as the COVID-19 pandemic has completely shifted the work landscape. A small percentage of the Federal government was previously authorized to work remote before the pandemic – the transition was a large test for agency resiliency. Now, some agencies have 80% of their workforce connecting to virtual desktops and the trend will likely continue for the foreseeable future.[1]
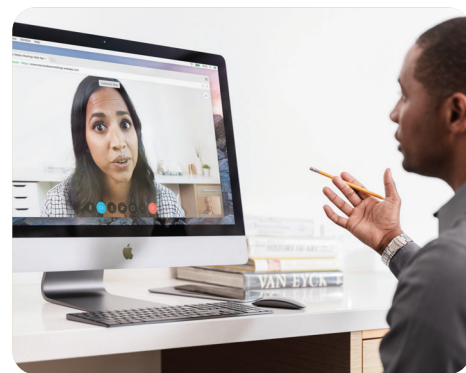
With guidance from the Office of Management and Budget, agencies adjusted to telework while ensuring best security practices.[2] While many agencies made investments in telework infrastructure over the past few years, some agencies were more prepared than others for the rapid shift. IT modernization efforts have been critical to the success agencies have found when forced to rapidly transition to remote work. To continue to deliver on the mission, IT departments need to focus on providing the right tools to employees.

Tools to Use

Utilizing the right tools to collaborate is important, and from February to April alone, agencies spent $288 million on teleworking products and services.[3] While agencies can no longer work together in person, online tools offer ways to unite applications and offer secure solutions. Agencies are heavily investing in: unified communication and collaboration tools, PCs and tablets, voice over IP, network upgrades, software licenses or cloud services, and additional cybersecurity solutions.[4] Working together to use modern technology and internet of things (IoT) devices to foster collaboration over the cloud helps ease the transition to the new normal.

Security Hurdles

As agencies adjust and utilize these new tools, they need to consider potential challenges and security protocols moving forward. Cybersecurity and privacy concerns are more prevalent when implementing new tools and bring higher risk of cyberattacks.

Like any online activity, good security hygiene and practices can help mitigate cyber risks. Offering training and guidance to employees on new tools and making sure they have proper privacy information controls in their homes is critical to keeping work environments secure. Virtual meetings can be secured from potential hacks by providing limited access codes, one-time PIN, multi-factor authorization, monitoring attendees, and disabling unnecessary features.[4]

Best Practices Moving Forward

It's important to keep communication open when employees are no longer in the same building to keep

---

1 COVID-19 drives agencies to investigate alternatives to VPNs, raises need for BYOD support
2 Memorandum For Heads of Executive Departments and Agencies
3 Spike in Federal COVID-19 Spending Flattens as Total Nears $3B
4 Preventing Eavesdropping and Protecting Privacy on Virtual Meetings

operations running smoothly and effectively – collaboration can lead to building closer relationships between employees and constituents. Cisco and ThunderCat Technology offer collaboration services to enable employees to continue to work from home and safely connect to their network and teammates regardless of location or device. The Cisco Unified Communications Solution offers answers to keep agencies engaged and efficient:[5]

Unite applications and endpoints
Unified Communications Manager delivers the right collaboration experience to any device, including voice, video, messaging, mobility, and web conferencing. Empower people to engage anywhere, using secure solutions.

Choose the right endpoints
Swap conference rooms with virtual meeting rooms, IP phones, and video systems that are integrated and affordable, with advanced capabilities.

Secure conferencing anywhere
Bring teams together with highly scalable voice, video, and content sharing. Protect from hackers and other cyber threats during telework, while avoiding the disruption of vital government services.

Move collaboration to cloud
FedRAMP-authorized collaboration and videoconferencing systems maximize flexibility. WebEx web conferencing offers support for meeting, events, and training, hosted in a secure environment.

---

[5] Unified Communications Solutions for Federal Government

For more information on how Cisco and ThunderCat Technology
can collaborate with your agency during these uncertain times, visit:
https://www.thundercattech.com/partners/cisco

THUNDERCAT TECHNOLOGY

CISCO
Partner
Gold Certified