Telework Hurdles Require Strategy and Culture Changes

As agencies prepare for mass telework, clear communication and an eye on security will minimize stress on employees.

James Mersol
Thu, 03/19/2020 - 16:29

The rapid spread of the novel coronavirus has created disruptions across the U.S. — not the least of which is to organizations, both public and private, who have to plan and implement strategies that keep their employees and their families safe while minimizing the impact on their missions.
Acting Director of the Office of Management and Budget (OMB) Russell Vought issued a March 17 guidance memo, directing agencies to “maximize telework across the nation for the Federal workforce (including mandatory telework, if necessary), while maintaining mission-critical workforce needs” and to “assess professional services and labor contracts to extend telework flexibilities to contract workers wherever feasible.” This memo was a shift in both range and intensity from OMB's March 15 memo, which only applied to agencies in the national capital region and outlined fewer specific recommendations for agencies to follow.

The Office of Personnel Management (OPM) also encouraged agencies to extend “maximum telework flexibilities” to workers in the national capital region March 16 and expanded that guidance to federal government offices nationwide March 19.

OMB acknowledges that this is a rapid and dramatic change in agencies’ operations, but emphasizes “agencies must take appropriate steps to prioritize all resources to slow the transmission of COVID-19, while ensuring our mission-critical activities continue.”

For many, even two weeks ago “feels like a million years ago,” said John Dickson, principal of Denim Group, an enterprise application security consultant based in Texas. From what he has seen, the readiness and capacity for remote work depends largely on the strategy and culture of each organization.

Teleworking policy at the federal level is delegated to each agency, out of a recognition that each agency has different requirements and considerations for its workforce. Some agencies, like the Consumer Financial Protection Bureau (CFPB), have moved to an agency-wide telework policy, while others, like the U.S. Citizenship and Immigration Service (USCIS) are adjudicating telework eligibility on a case-by-case basis.

Agency policies on telework are “evolving and changing every single minute,” said Mika Cross, vice president of employer engagement at FlexJobs, a job-search site for remote and telework employment opportunities.
Cross, who has spent her career both in and outside of government helping organizations manage their employee programs, recommended that agencies think about the policies not just for the immediate future, but also more broadly. Many of the terms at play, such as “maximum flexibility” and “telework eligibility” lack a clear, common definition that serves as the basis for agency workforce policies. Cross encourages agencies to not only decide upon these definitions, but also to incorporate them as part of agencies’ continuation of operations planning (COOP), procedures that each agency is required to have in place for emergencies and other abnormal circumstances.

Moreover, Cross recommended, telework eligibility could be written into employees’ contracts. Even if an employee does not telework frequently, a requirement to telework at least once a month gives them practical experience in how to carry out their duties remotely with minimal disruption. In the short term, Cross said that internal agency resources could help ease the transition to mass telework.

“There’s a learning curve,” Dickson said, for those unaccustomed to telework. Even virtual private network (VPN) access is “an outgrowth of the culture.”

Secure VPN access for agency-wide telework has been an early concern as more and more agencies move to telework. While VPNs offer a relatively secure way to access agency servers and networks remotely, they tend to be slower and less secure than an on-prem connection. Most public and private organizations have VPNs set up for the number of employees who might need remote access at any given time, but few have tested access for most or all employees simultaneously.

In its March 6 advisory on managing cyber risks during the COVID-19 pandemic, the Cybersecurity and Infrastructure Security Agency (CISA) urged agencies to “ensure [VPN] and other remote access systems are fully patched,” citing its January alert about potentially compromised VPNs.

“A remote, unauthenticated attacker may be able to compromise a vulnerable VPN server,” the alert explained. “The attacker may be able to gain access to all active users and their plain-text credentials. It may also be possible for the attacker to execute arbitrary commands on each VPN client as it successfully connects to the VPN server.”
“This vulnerability has no viable workarounds except for applying the patches provided by the vendor and performing required system updates,” the alert stressed. Routine patching is the best method to maintain VPN security as adversaries look to exploit weak links during the early phases of mass telework.

“Implement MFA [multi-factor authentication] on all VPN connections to increase security,” CISA encouraged in official guidance March 13. The agency encourages IT personnel to test VPN bandwidth and other potential limitations in order to make informed decisions about how to best ensure continuity of operations during mass telework.

CISA also advised everyone to be on the lookout for phishing and other scams related to COVID-19. Cybersecurity firm CrowdStrike noted that it has seen a rise in COVID-19-related scams in recent days during a March 18 call, underscoring that “continued education is critical.”

Even organizations who had the luxury of running a pilot program for mass telework two or three weeks ago found that not every speedbump could be easily smoothed over. One source said that their accounting office found it difficult to access their financial systems easily and that some processes, like printing, signing and issuing checks, had to be done in person.

One way to mitigate the impact to operations from these in-person tasks, Cross suggested, is to establish staggered work schedules, something that the Defense Department has established. Teams should communicate with facilities to establish schedules for workspace sanitization and in-office work, even if that is limited to tasks that can only be performed on site.

Some aspects of telework policy, like establishing alternative work schedules where needed and continuing education over phishing activity, will take time for agencies to enact. This process should be built upon a foundation of “accountability, accessibility and open and transparent communication," Cross said.
While it may be difficult for agency leadership to delegate responsibilities to managers and their teams, especially remotely, Cross said that leveraging collaborative measures, like creating a buddy system for minor obstacles, can help teams work through difficulties in telework. Most employees’ work responsibilities include “other duties as assigned,” Cross noted, and these duties could include taking the lead on learning how to implement new communication platforms or finding ways for teams to align responsibilities as work schedules change.

Agencies should also foster a “culture of support” where employees can work with their managers to find solutions to their challenges, such as caring for sick relatives or homeschooling children during the pandemic. These situations do not normally mesh well with a 9-to-5 workday, but by leaning on employee assistance programs and other resources, teams can find a mutually agreeable solution.

Currently, “the number one focus is for you and your families to be healthy and safe,” Dickson said.

View printer friendly version

coronavirus
Federal Workforce
Federal Government Telework
USCIS
Federal Cybersecurity
Standard