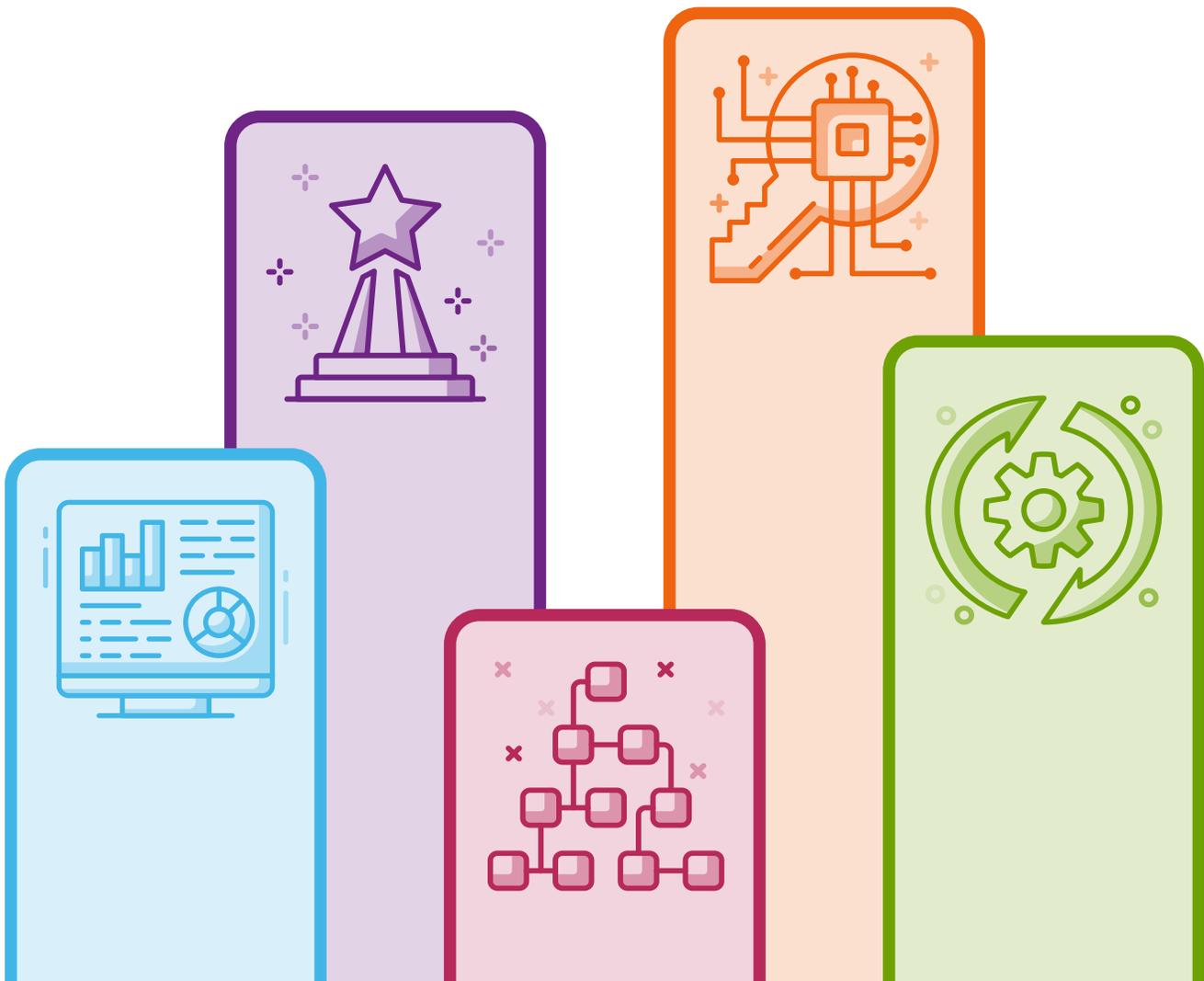


# 5 Pillars for Cultivating a Secure and Inclusive Hybrid Workplace

**DELL** Technologies



carahsoft.



# Contents

- 3 Executive Summary
- 4 The Hybrid Workplace at a Glance
- 5 Government in Transition: From Remote Work to the Hybrid Workplace
- 7 5 Pillars for Building the Hybrid Workplace of the Future
  - Data
  - Innovation
  - Modern Infrastructure
  - Zero Trust Cybersecurity
  - Backup and Recovery
- 14 Laying a Foundation for the Hybrid Workforce
- 16 10 Tips to Better Support Employees in a Hybrid Workplace



# Executive Summary

Agencies at all levels of government are at sea, navigating relentless waves of new policies, technology demands and workforce changes with what can often feel like paddle-boat resources.

They know they need to modernize their operations. And, yes, Congress has provided an unprecedented level of funding to support those efforts. The [Technology Modernization Fund](#) provides financial resources for federal agencies, and the [American Rescue Plan](#) does the same for state and local ones.

Still, the experience of the past year and a half has made agencies rethink their modernization strategies. Government offices may be reopening, but the workplace will never be the same. **Most agencies need to create a flexible, hybrid workspace for the long-term — one that enables employees to work effectively no matter where they are located.**

Getting there won't be easy. Though government agencies responded with remarkable speed and agility to COVID-19 -- taking emergency measures that enabled thousands of workers to continue doing their jobs at home -- a traditional, office-centric culture still pervades. Changing that culture permanently is going to be difficult.

Having gotten through the initial crisis, agencies now seek to navigate a course that will transform government in the long term. The uncertainty of the present moment won't make the journey any easier. If they succeed, their destination will be a hybrid workforce that does the work of government better than it's ever been done.

This guide, based on the recent GovLoop, Dell Technologies and Carahsoft Virtual Summit, "[How to Support the Hybrid Gov Workforce](#)," will provide agencies with insights into the technologies and strategies that can help them move into this new environment.

# The Hybrid Workplace at a Glance

The White House announced in a [June 10 memo](#) that federal agencies could extend flexible schedules and [remote, hybrid work arrangements](#) to employees in the post-pandemic era.

The prevalence of remote work among federal employees shot up 1,900% during the pandemic — from 3% of federal employees who worked remotely before the coronavirus outbreak to nearly 60% of employees who reported [working somewhere other than their office](#) at the peak of the crisis.

Eighty percent of federal and Washington-based government employees reported that [productivity increased](#) while teleworking during the pandemic. If leaders fail to acquire [digital communication tools](#) and train hybrid teams to optimize their use, they aren't equipping those teams for success.

***“There’s a strong link between [telework participation](#) and engagement scores [of employees]...and it’s the same with [satisfaction and health and safety.](#)”***

**Kimberly Wells**

Acting Director of Strategy and Innovation, OPM

One [study](#) found that 65% of working women said the pandemic has made things worse for women at work.

Jeff Neal, a former Chief Human Capital Officer (CHCO) at the Department of Homeland Security, told National Public Radio that half of the federal workforce — about a million workers — have jobs that are [conducive to working from home](#). The workforce of the future is probably going to be a hybrid, “somewhere between what we had pre-pandemic and what we have now,” he said.

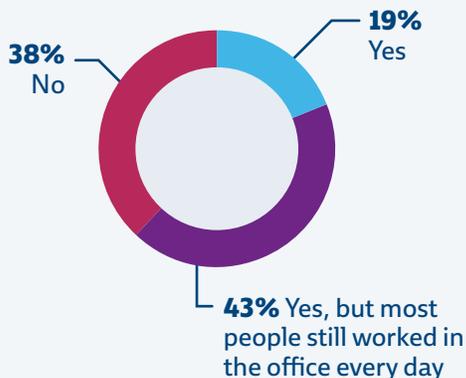
The Biden administration has directed agencies to [train managers on fair and equitable performance management for hybrid teams](#). This includes raising awareness among supervisors that evaluation of an employee’s performance:

- Should be based on factors such as accountability for results or quality of the work
- Should not be affected by whether an employee is working in the office, teleworking, based remotely or working a flexible work schedule.

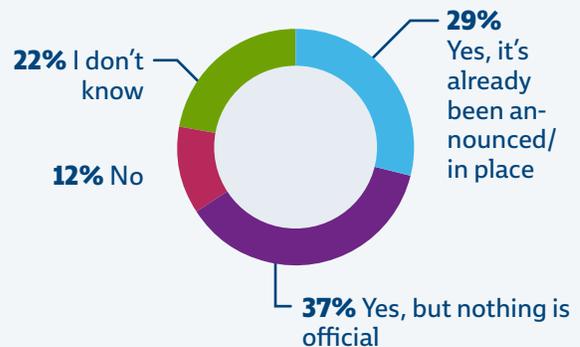
Post-pandemic, 32% of employees say they [never want to return to working in the office](#). At the other extreme, 21% never want to spend another day working from home.

*Here’s how the GovLoop community responded to a [May 2021 survey](#) about hybrid work:*

**Prior to COVID-19, did your organization have a hybrid workforce?**



**Do you think your agency will adopt a hybrid workforce this year?**



# Government in Transition: From Remote Work to the Hybrid Workplace

## KEY TAKEAWAY

Keep the focus on the people, not just the technology. Hybrid work environments will seek to maximize the return on investment in agencies' workforces, wherever workers happen to be. But that should not come at the expense of supervisors considering some key issues.

**A  
Conversation  
With:**



**Traci  
DiMartini**  
GSA



**Jenny  
Rostami**  
GSA



**Sherry  
Van Sloun**  
ODNI

Early in the pandemic, some federal managers couldn't understand why their teams weren't eager to attend the boss's standing two-hour staff meeting. Even now, some managers continue to pine for pre-pandemic workflows.

"They're chomping at the bit to get everyone back into the building," said Traci DiMartini, CHCO at the General Services Administration (GSA).

In reality, government workers and managers must accept that the good old days are gone for good. COVID-19 has been both a tipping point toward and an accelerant of hybrid work.

***"We are completely rethinking how government works and delivers services — how we recruit, retain and attract people into the workforce," DiMartini said. "We are upending the normal truths and norms that we held dear."***

## Bureaucracy vs. Empathy

As the hybrid workforce grows, decentralized offices will need leaders who are insightful and intuitive. "During the pandemic, we saw an increase in managers focusing more on emotional intelligence, communication skills and having hybrid teams work together," DiMartini said. "There was more inclusivity."

Sherry Van Sloun, Assistant Director of National Intelligence for Human Capital at the Office of the Director of National Intelligence, agreed. "Leadership in the intelligence community has been flexible, creative and empathetic," she said.

## Burnout

Managing hybrid workforces can be challenging. For example, burnout is becoming very real, said Jenny Rostami, Acting Executive Director for the Centers of Excellence at GSA. Good leaders used to be able to spot burnout on their workers' faces. Reading the room when you're online is much more challenging.

But there is no one-size-fits-all solution. "The introverts are starting to feel really comfortable with working from home, and the extroverts are starting to feel like they're going to burst at the seams if they don't go back to an office," Rostami said.

## Rigidity vs. Flexibility

For decades, flexible work options for federal jobs were limited. The pandemic forced a change in policy.

Even as agencies bring people back to traditional offices, they will “continue to offer flexibilities that I don’t think we ever really pushed on before COVID hit,” Van Sloun said. “We’re excited to start piloting some ideas that we probably wouldn’t have done as fast as we have.”

## Metrics, Old and New

The hybrid workforce is upending processes and recalibrating metrics. Supervisors who in the past measured productivity by how many people were in the building need new ways of measuring success, DiMartini said.

**“We’re going to see a reinvestment in how we train supervisors in performance management,” she said. “Everyone has to understand [that] with increased flexibilities come increased levels of accountability.”**

## Equity

Managers in a hybrid environment must guard against inequality, real or perceived, that could divide remote workers and in-office colleagues. “We have to make sure we’re treating each other fairly across performance management cycles, to include promotions and bonuses,” Van Sloun said. “That’s going to be critical to making this hybrid workforce work.”

**“We have to create an inclusive environment where location does not exclude you from being at the table,”** Rostami said.

## IT Deficits

Agencies that had leaned into telework before the pandemic will have an easier with the transition to a true hybrid workforce.

“We’ve always embraced telework and our IT infrastructure,” GSA’s DiMartini said. Agencies that have stumbled while trying to keep people connected “were too afraid to make those IT investments or they didn’t prioritize them.”

No agency is immune to setbacks, though. **“At NASA we can go to the moon,” an employee of the space agency said, “but we struggle with Zoom.”**

## Human Deficits

“It’s not really the technology that makes anything fail,” Rostami said. The success or failure of hybrid work will rise and fall on a fulcrum of workers.

“I’ve seen efforts with millions of dollars that don’t get the adoption warranted because stakeholders were not at the table,” Rostami said. “I think the biggest lesson we’ve learned has definitely been people first.”

## Private Lessons

The public/private gap that existed before the pandemic is no longer sustainable.

An intelligence community program will deploy human resources officers to for-profit companies to learn how they do business, to look at their innovation and to help the office be more innovative and creative, Van Sloun said.

“We have to start enabling the public to interact with the federal government in the same way they do privately,” Rostami said.

## Looking Ahead

“We’re in this together,” Van Sloun recalls employees often reminding themselves at the beginning of the pandemic. “Those words are just as important now.”

As hybrid workplaces become more prevalent, employees should remember that people have been through a lot. “Be respectful to your colleagues,” she said. “We don’t always know the sorrow, the grief, anxiety or fear that someone else is carrying.”

“It’s OK to not have all of the answers right out of the gate, but as long as we work as a community, hold ourselves accountable and take care of our people, those are the things that matter most. Everything else will fall into place,” DiMartini said.

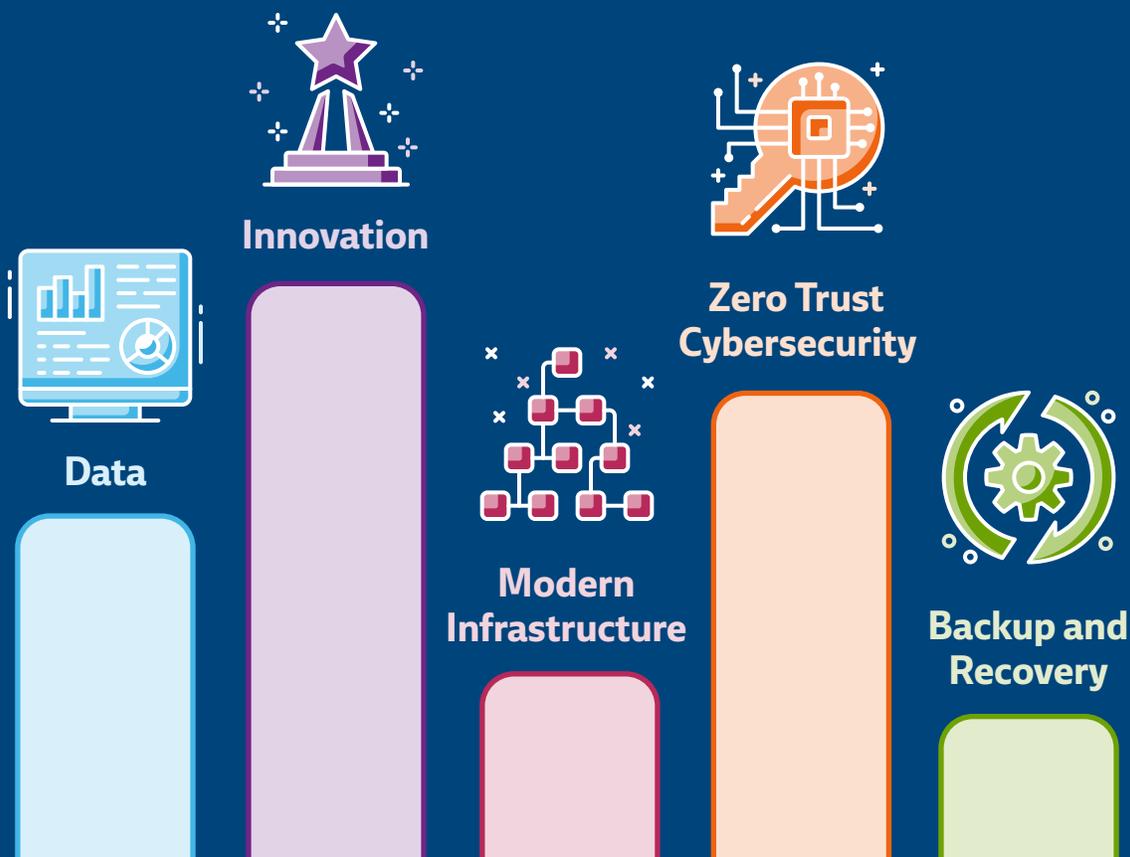
# 5 Pillars for Building the Hybrid Workplace of the Future

Born of necessity, the evolving vision of a federal hybrid workplace that has emerged during the COVID-19 pandemic has the potential to revolutionize how government operates.

Enabling large numbers of employees to work remotely will require investments in IT, flexible leadership strategies, new policies and major cultural shifts. If done well, those investments and initiatives could fundamentally change the way agencies:

- Hire and manage employees
- Interact with and deliver services to customers
- Attain mission goals

To realize these and other benefits, agencies must prioritize five key pillars of the hybrid workforce. We explore each of them in the following pages:



# PILLAR 1

## Data



**Chris Ritter**  
Dell Technologies



**Chakib Chraibi**  
NTIS



### The pandemic taught agencies lessons about data that will inform operations and mission attainment for years to come.

For example, research teams displaced from traditional workplaces were able to track and research COVID-19 using government data in an unprecedented way.

“The challenge was to disseminate data for 1,000 different individuals and access points from remote locations,” said Chris Ritter, a Principal Engineer and Chief Application Architect at Dell Technologies Public Sector.

Using data accessed remotely, pandemic fighters created a living template for how government agencies could pursue data-critical missions in coming years. As a hybrid workforce becomes the norm and data-driven decision-making becomes more prevalent, reliable access to quality data will become a backbone of effective governance.

The pandemic forced an acceleration in digital transformation in government, said Chakib Chraibi, Acting Associate Director for the Office of Data Services and Chief Data Scientist at the National Technical Information Service.

## Data Policies

The pandemic reinforced the importance of using data to pursue agencies’ missions. Recent federal initiatives provide policy support for accelerating the use of data as a strategic tool. Those include:

- [The Foundations for Evidence-Based Policymaking Act of 2018](#)
- [The Federal Data Strategy](#)
- [The National Artificial Intelligence \(AI\) Initiative Act of 2020](#)

“Federal agencies are looking to increase their use of data as a strategic asset,” Chraibi said.

## Data Architecture

Agencies must be willing to reevaluate misconceptions about modernization and data frameworks. During the Cloud First era, for example, cloud migration was considered an end unto itself, rather than the means to better data management. The fallacy persists, Ritter said.

“Organizations are rushing to throw data into the cloud with the assumption that it will be cheaper or easier to access,” Ritter said. “Accessing data isn’t necessarily easier when it’s scattered in the cloud across different platforms and protocols and cost-based service levels.”

## Data Location

A better strategy is to meet data where it lives, that place where a high percentage of data is generated, stored or accessed. That could mean accessing information, whether generated by an Internet of Things device or a remote worker’s laptop at the edge, instead of always funneling data to centralized storage before accessing it. “The right architecture provides benefits of private and public cloud to the edge,” Ritter said.

Before committing to a data architecture, however, agencies should understand users’ data requirements, how they access data, users’ data governance, security and compliance policies, data flow, and physical considerations.

Advanced IT capabilities are fundamentally rooted in data, Chraibi said. “Getting the right information to the right people at the right time and in the right place is essential to data-driven decision-making and to supporting analytics capabilities that deliver mission outcomes,” he added.

## Develop a Roadmap

Agencies must build data frameworks that are flexible, scalable and capable of supporting robust data strategies.

“It’s essential for federal agencies to develop a roadmap for a consolidated and streamlined approach for data collection, discovery, management and dissemination to empower not only basic data analytics, but really deep analytics for the long term,” Chraibi said.



## PILLAR 2

# Innovation



**George Strother**  
USDA



**Cameron Chehren**  
Dell Technologies



**At a time when government agencies need innovation more than ever, the growth of a hybrid workforce can complicate the adoption of innovative practices, because so many of the existing practices are built around the physical workplace.**

But it can be done. Following guidelines from the public and private sectors, IT experts can help agencies overcome institutional inertia — and nurture innovation.

### Training

Technology evolves faster than the people who use it, making change management a critical component of IT advancements that promote innovation.

“Training and mindset are probably the most important pieces that organizations will have to overcome,” said George Strother, Storage Management Branch Chief at the Agriculture Department’s Office of the Chief Information Officer for the National IT Center. “We’re going through a big technology transformation right now. Getting past the fear of change is really important.”

Strother recommended several resources to address the mindset challenge:

- [“Site Reliability Engineering: How Google Runs Production Systems”](#)
- [“The Phoenix Project: A Novel about IT, DevOps, and Helping Your Business Win”](#)
- Linux Academy training

### Apps

Strother encourages agencies to invest in new tools, such as Microsoft Teams, shared knowledge stores and videoconferencing, which promote collaboration across traditional offices and remote workplaces, instead of just relying on email.

“Collaboration platforms become the crucial means of communication. Whether people are in the office or a coffee shop, these tools help workers to accomplish what they need to accomplish,” Strother said.

### Cultural inclusion

Cameron Chehren, Chief Technology Officer (CTO) and Vice President of Presales Engineering at Dell Technologies Federal, said that intangible factors matter a great deal in being able to create a culture of innovation.

The foundation of innovative culture is organizational inclusiveness — listening to everyone. “You may not accept or adopt all recommendations, but the fact that everyone’s ideas are included is vitally important,” Chehren said.

Innovative organizations recognize the value of employees for more than just their technical expertise, acknowledgement that neutralizes fear about IT and paves the way for innovation. “People’s value increases in innovation environments because they are familiar with mission and mission outcomes, especially in government environments,” Chehren said.

Innovation is all about relationships — with community partners and technology providers — and rallying everyone behind the common vision of advancing the mission. “If you use that lens first, rather than a technological one, you’ll see change happen rather quickly,” he said.

### Automation

Bringing automation into the workplace sometimes stokes fears of job loss. Often, automation benefits employees by scaling human potential, Chehren said. “Automation was always my friend,” he said. “We use it for managing storage, databases and servers. It’s how you function today as an enterprise.”

Mission requirements are exponentially exploding and budgets aren’t keeping pace with demands, making automation a force multiplier right now. Before virtualization, an administrator could typically manage 10 devices. Today, it’s thousands, he said.



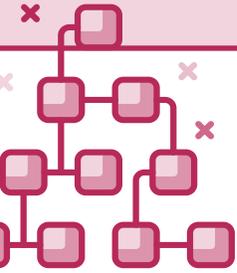
# Modern Infrastructure



**Steve Tuomey**  
Dell Technologies



**Frank Indiviglio**  
NOAA



**Most weeks, an Air National Guard training center in Pennsylvania welcomes hundreds of engineers who undergo intensive training to understand the service's aircraft.** In the

past, as soon as one group completed its training on a Thursday, the center's IT staff began reconfiguring the training technology before the next cohort's arrival. "They would spend all day Friday and most of the weekend reimaging and rebuilding everything manually," said Steve Tuomey, Data Center Compute Executive at Dell Technologies Federal. "It took almost three days to complete."

Seeking a better way, Tuomey recommended that the center introduce a hyperconverged infrastructure (HCI) solution and 500 virtual desktops, eliminating the need to touch every single server, PC and workstation between training sessions. HCI provided new efficiencies that freed the IT staff to work on other tasks.

## Overcoming barriers

If HCI can slash weekly transition times at an Air National Guard training center, what can it do for agencies that are trying to create a more efficient hybrid workforce?

HCI brings together into one appliance-like platform system components — compute, networking, storage and security — that in traditional IT have existed in separate silos, Tuomey said. "Hyperconverged allows formerly siloed teams to work without barriers. They collaborate easier, better and more efficiently."

## Tools for efficiency

Frank Indiviglio, Deputy Director for High Performance Computing and Communications at the National Oceanic and Atmospheric Administration (NOAA), said HCI helps agencies shift their focus from organizational operations to services and, ultimately, mission attainment.

"HCI in the government is a way to simplify how we manage our resources. It shifts our management away from worrying about parts in the data center to managing the data center more as a whole through services and applications," Indiviglio said.

That shift enables agencies to be more flexible and to adapt to changing workloads. For instance, NOAA is using AI and machine learning, particularly in its HPC line of service. (The efficiencies and scalability that HCI provides facilitate the adoption of high-performance computing and the use of AI, IoT and software-defined storage.)

"It allows us to incorporate new edge computing cases and new workloads more rapidly," Indiviglio said. "It gives us flexibility, not only to adapt but to add value."

## Foundation for modernization

HCI is a tool for adopting modern IT processes. Its flexible infrastructure and built-in failure-recovery features enable agencies to move development teams more aggressively into DevOps and DevSecOps, Indiviglio said. "Those types of workflows become easier to implement when your infrastructure is common and converged."

For example, NOAA's HPC users get the same level of HPC service regardless of location.

"They don't have to worry about accessing the right resource," Indiviglio said. "They can build what they need and not worry about the base level of services."



## PILLAR 4

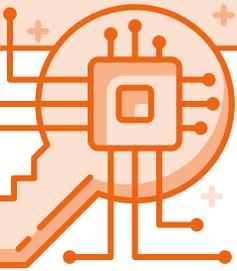
# Zero Trust



Vijay  
D'Souza  
GAO



Dan  
Carroll  
Dell  
Technologies



### Before the pandemic, the Government Accountability Office (GAO) adopted a collaboration tool for facilitating workflows in traditional offices.

When the pandemic sent everyone home, the agency discovered the tool lacked the robust audio and video capabilities homebound employees needed. The gap wasn't just an inconvenience; it was a potential security issue.

"The security issue is that you risk your staff using third-party tools that aren't secure because they're not satisfied with the tools they're getting through their workplace," said Vijay D'Souza, Director of GAO's IT and Cybersecurity Team.

The pandemic essentially added another layer of complexity to cybersecurity.

### Executive Order

An [executive order](#) President Biden issued in May calls for stronger cybersecurity of federal networks.

"The order drives home the importance of shifting to a model where you focus on securing your most critical data," D'Souza said.

Dan Carroll, Cybersecurity Practice Lead for the Office of the CTO at Dell Technologies Federal, said the executive order and the recent spate of high-profile cybersecurity breaches, including the Colonial Pipeline ransomware attack, are calls to action.

"Cyber warfare is here," Carroll said. "There's a need for federal agencies to do more to protect our critical infrastructure. The executive order gives direction to agencies."

### Barriers

Implementing a [zero trust architecture](#) and securing a hybrid workforce requires overcoming technical and cultural impediments. Agencies frequently focus on thwarting sophisticated "super high-end infiltration," for example, while missing basic security principles, Carroll said.

"When we audit federal agencies, there's always a lot of attention paid to new zero day vulnerabilities and high-profile stuff, but we're finding critical vulnerabilities that have been known about for years," D'Souza said. "Basic cyber hygiene isn't followed. Agencies don't have an accurate inventory of devices that are connected to their network."

Visibility, or seeing the whole field, remains a challenge. Being able to easily analyze systems and get a view of the total infrastructure should be a priority, Carroll said.

Agencies can also segment networks to limit attackers' lateral movements. Agencies should review their data backup strategies because "without an effective backup strategy, you can't have data trust, which is a tenet of zero trust," he said. "Encrypt everything."

### Integration

D'Souza advises agencies to be strategic when complying with the administration's executive order and pursuing a zero trust architecture. Specifically, that entails integrating new initiatives into existing security programs and efforts.

"There's never going to be enough money, so prioritize and start where you will get the most bang for your buck," D'Souza said.

### Embrace Momentum

"COVID probably accelerated remote work for the federal government by at least a decade," Carroll said. Don't kill momentum by starting over with cybersecurity.

"Don't blow up all of your current plans," he added. "Leverage existing assets. Customers don't realize how many security features and capabilities they have within existing solutions that will help with reporting on zero trust goals."



## PILLAR 3

# Backup & Recovery



**Gregg Tremi**  
HHS



**Robert Tagalicod**  
HHS



**Brad Montgomery**  
Dell Technologies



**The growth of a hybrid workforce underscores the need for data integrity and accessibility for all employees – wherever they're located.**

Cyberattacks occur somewhere in the world every 11 seconds, causing global impacts in the first half of 2021 in excess of \$6 trillion.

"It's not a matter of if you'll have a cyber event, it's when," said Gregg Tremi, Assistant Inspector General for the Office of Management and Policy and the Office of the Inspector General at HHS.

### Get Ready, Now

Data protection rule No. 1: Your data, your responsibility.

"There's a misconception that the cloud provider retains responsibility for the protection of customer data," said Brad Montgomery, Director of Presales Engineering for Federal Data Protection Solutions at Dell Technologies.

Robert Tagalicod, Chief of Cyber Communications and Engagement at HHS's Office of Information Security, suggested that "collaborative preparedness" is key to surviving a data crisis with minimal disruption. "All employees should have critical awareness in real time to understand threats," Tagalicod said.

### The experts further advised agencies to:

- **Harden their most vulnerable assets** (human workers) by providing more training, education and strategic hiring of key personnel.
- **Prepare for worst-case scenarios** in which agencies need third-party help. "Who would you call?" Tremi asked.
- **Identify datasets, data types, applications, databases and foundational technologies** needed to restore operations.
- **Review peripheral technologies and applications** that can contain threats, as the SolarWinds cyberattack demonstrated.

### Tools and Resources

A shortage of qualified IT workers can diminish agencies' efforts to protect data. But agencies can use private-sector organizations to supplement in-house staff. "It has to be a hybrid approach between federal oversight and the right private-sector organizations...to supplement us as we're doing our oversight work," Tremi said.

Montgomery encouraged agencies to consider use of a "cyber vault" that preserves copies of the agency's most critical datasets to expedite a recovery.

A cyber vault is last-resort storage because regular backups are susceptible to sophisticated cyber attackers, Montgomery said. "Once it's gone, there is nothing to protect the production network."

### Preparedness in a Hybrid World

With the administration's cybersecurity executive order in place and the concept of zero trust ratified as a sanctioned IT security philosophy, what actions should agencies take in the coming year?

Agencies with disaster recovery plans should also adopt cyber resilience plans that would enable them to recover from all forms of data destruction, Montgomery said.

In addition, agencies must better operationalize the concept of zero trust architecture via DevSecOps, Tagalicod said. "Security should be part and parcel of our thinking at the beginning of any architecture."

Tremi's advice: "Make sure your cyber plan is in place and that it weaves in nicely with your disaster recovery plans. It's important to be prepared for a data crisis. We know it's coming."



# Accelerate Transformation

To meet the variety of missions you encounter every day, you need responsive IT. Dell Technologies offers federal agencies the technology expertise, end-to-end solutions and world-class service you need to be prepared for what comes next.

[DellTechnologies.com/Federal](https://DellTechnologies.com/Federal)

 **Dell** Technologies

# Laying a Foundation for the Hybrid Workforce

**Creating a flexible, scalable and secure IT environment from a lumbering legacy IT system isn't easy, but it can be done.** Arveen Kohli, Senior Manager for Civilian Services Sales at Dell Technologies Federal, recently spoke with GovLoop about guiding organizations through digital transformations.

## GovLoop: Why are government agencies seeking flexible, scalable, secure IT environments?



**Arveen Kohli:** Agencies have a lot of data they could use to deliver outcomes. They want a model that allows them to leverage processes and workflows in an agile way to speed delivery of outcomes.

## So, data is the crux of the issue?

There's a lot of data sitting on obsolete infrastructure. How are you going to drive outcomes when you don't know what's in your application data, your datasets or your overall data footprint?

## What are the characteristics of modern IT environments?

Achieving a flexible, scalable, cloud or multi-cloud footprint is a matter of transforming people, processes and organization to achieve mission outcomes. You change the DNA of an organization to operate in new ways. At Dell Technologies, we create a platform strategy that allows for flexibility, scalability, agility and the ability to manage that in a sustainable way.

## How do you move those pieces forward in unison?

You bring along people and processes together. You never do one without the other. People must move into roles that allow them to provide optimal performance in a modernized, multi-cloud era.

Will your people manage these multifaceted cloud platforms? Or will you pick a partner to manage them for you? Most agencies want to control different facets of cloud platforms. For that to happen, people must have cloud-specific roles.

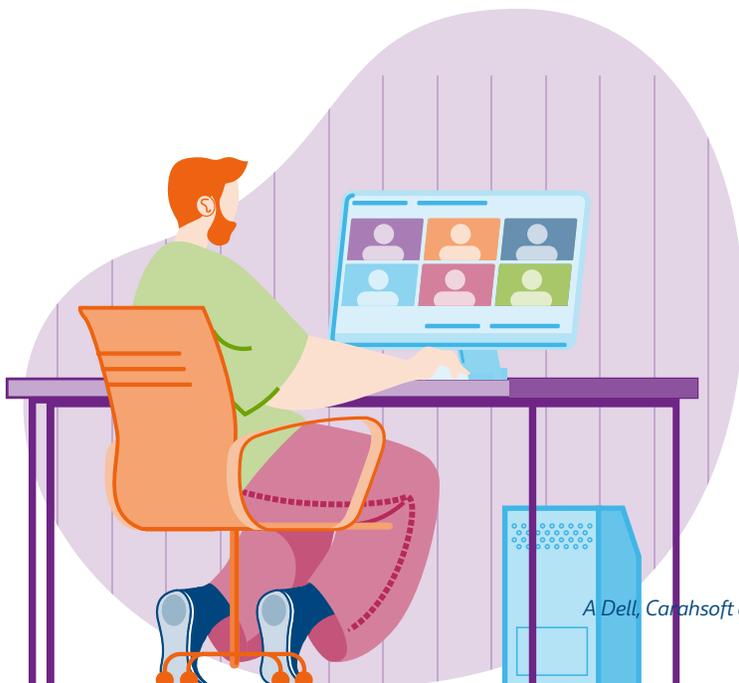
## How do you make the transition?

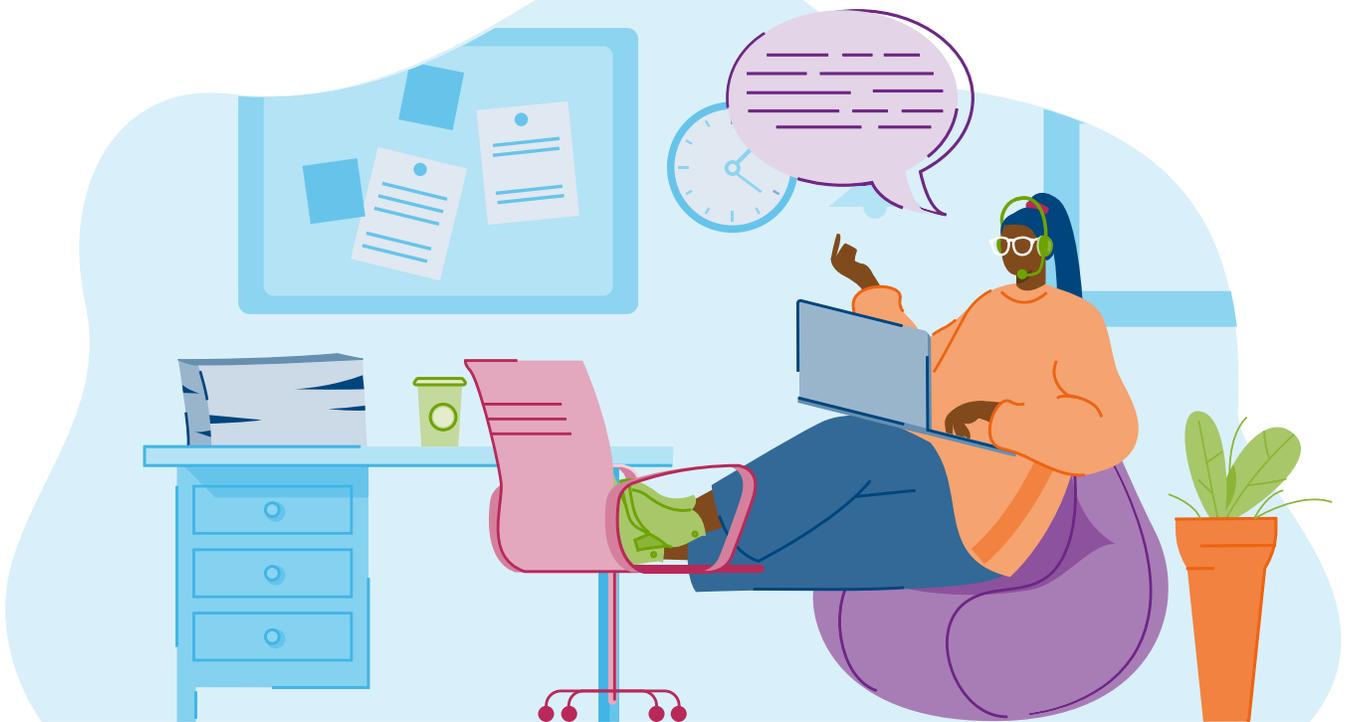
Don't try to boil the ocean. Small, swift wins are more in alignment with a scalable, swift and efficient cloud model than trying to get everything changed at once. Aligning transitions to missions and outcomes helps to justify use cases. Build financial optimization models and efficiencies around making things happen.

There are different ways to convert legacy systems. You can do this by maintaining applications in an existing environment, re-platforming them to a new environment, having a multitiered hybrid cloud, shifting portions of multitier applications to a public cloud, refactoring them, modifying applications to a new environment on premises or in the cloud, developing for the cloud your cloud-native applications, or moving to a Software-as-a-Service version of the package staff model.

## What's propelling the uptake of modernized IT environments?

Most important is security, which goes hand in hand with data. If you don't have a handle on everything in your ecosystem, you can't secure it. Understanding your data footprint reveals what's redundant, what you're not using and what's obsolete. Data clarity fuels security.





### **Has the pandemic changed how agencies think about IT modernization?**

I think it changed how each of us thinks about how we do things. It taught us to plan for today, not five years from now. Planning for three to 18 months is more realistic and achievable. Two, we need a handle around data so that when we're driving outcomes, we're also developing the framework for zero trust and security.

### **How will these new environments improve workers' effectiveness, wherever they are located?**

The dynamics of a flexible workforce redefined themselves over the last year and a half. We learned that we have the technology to support remote work. At Dell Technologies, we are packaging laptops for customers in a way that is application-mobility-driven and persona-driven. When you open your laptop, you see only the applications that you're supposed to access.

On the data center side, it's the same story. The multi-cloud, flexible cloud is so important because agencies and workers are operating anywhere and everywhere. Access drives success. It's important to deliver agility, efficiency and scalability to support programs in the most robust and efficient way.

### **What's the risk when agencies fail to acquire flexible, scalable and secure IT environments?**

There is a presidential [executive order around zero trust and the framework of security](#). Developing a secure

framework is like constructing a home to protect against intruders knowing that there will be intruders. That's why it's important to identify the data that lives in that home.

### **What are the three most important things that any agency can do to modernize its IT environment?**

One, know your application footprint. Are applications performing well or would a different platform improve performance? Two, what are the drivers for your mission over the next three to 18 months and are you in a position to attain desired outcomes? Three, focus on what is here today. Reanalyze your security footprint.

### **Change is hard. How do you get people to accept a new platform?**

More than 80% of IT modernization failures happen because people don't want to change the way they do things. It's extremely important to rearchitect the framework of roles and responsibilities in an organization when you do infrastructure or technology modernization. You want your people to be excited about changes.

### **Any parting words of wisdom?**

Don't adopt a technology-first mindset. Understand what you're driving towards and build your strategy for a multi-cloud, hybrid cloud. Have two or three public cloud providers and a private cloud provider. Adopt a cloud model that has the flexibility to scale back when needed.

# 10 Tips to Better Support Employees in a Hybrid Workplace

## People

1. **Put People First.** Employees determine the success or failure of any IT solution, not the other way around. Work to get employees' support.
2. **Lead with Empathy.** Building strong hybrid workforce teams will require talented leaders with highly developed emotional intelligence and communication skills.
3. **Be Fair.** For hybrid workplaces to succeed, managers must ensure equal treatment of all employees, regardless of where they're located.

## Process

4. **Cultivate Inclusiveness.** Listening to everyone in a hybrid work environment helps create a culture of innovation, said Cameron Chehreh, CTO, Dell Technologies Federal.
5. **Carpe Hybrid.** In response to the pandemic, agencies are rethinking how government works and delivers services, said Traci, DiMartini, GSA's CHCO. Don't miss the boat.
6. **Work Smarter.** Jettisoning legacy technology and manual workflows gives staff more time to work on other tasks, said Steve Tuomey, a Dell Federal executive.

## Data

7. **Elevate Performance Matters.** Hybrid work environments should focus on performance metrics, because with increased flexibilities come increased levels of accountability.
8. **Do Data Better.** Building agencies' capacity for using data as a strategic asset will advance hybrid workforces' effectiveness.

## Technology

9. **Own Your Security.** "There's a misconception that the cloud provider retains responsibility for the protection of customer data," said Brad Montgomery, data protection expert, Dell EMC.
10. **Think Like a Cyber Warrior.** "There's a need for federal agencies to do more to protect our critical infrastructure," said Dan Carroll, cybersecurity lead, Dell Federal.



carahsoft

DELL Technologies

***Thank you to Dell Technologies and Carahsoft for their collaboration on this resource for public sector professionals.***

### About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector. For more information about this report, please reach out to [info@govloop.com](mailto:info@govloop.com).

[govloop.com](http://govloop.com) | [@govloop](https://twitter.com/govloop)



1152 15th St. NW Suite 800  
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

