S. Hrg. 116–283

# MODERNIZING TELEWORK: REVIEW OF PRIVATE SECTOR TELEWORK POLICIES DURING THE COVID–19 PANDEMIC

## HEARING

BEFORE THE

SUBCOMMITTEE ON
REGULATORY AFFAIRS AND FEDERAL
MANAGEMENT

OF THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

JULY 28, 2020

Available via http://www.govinfo.gov

Printed for the use of the Committee on Homeland Security
and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
41–324 PDF WASHINGTON : 2020

## COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
MICHAEL B. ENZI, Wyoming
JOSH HAWLEY, Missouri

GARY C. PETERS, Michigan
THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

Gabrielle D'Adamo Singer, *Staff Director*
David M. Weinberg, *Minority Staff Director*
Zachary I. Schram, *Minority Chief Counsel*
Laura W. Kilbride, *Chief Clerk*
Thomas J. Spino, *Hearing Clerk*

## SUBCOMMITTEE ON REGULATORY AFFAIRS AND FEDERAL MANAGEMENT

JAMES LANKFORD, Oklahoma, *Chairman*

ROB PORTMAN, Ohio
MITT ROMNEY, Utah
RICK SCOTT, Florida
MICHAEL B. ENZI, Wyoming

KYRSTEN SINEMA, Arizona
THOMAS R. CARPER, Delaware
JACKY ROSEN, Nevada

Chris J. White, *Staff Director*
James D. Mann, *Senior Counsel*
Eric A. Bursch, *Minority Staff Director*
Jackie A. Maffucci, *Minority Policy Advisor*
Mallory B. Nersesian, *Subcommittee and Document Clerk*

# CONTENTS

## WITNESSES

### Tuesday, July 28, 2020

## Alphabetical List of Witnesses

## APPENDIX

# MODERNIZING TELEWORK: REVIEW OF PRIVATE SECTOR TELEWORK POLICIES DURING THE COVID–19 PANDEMIC

## TUESDAY, JULY 28, 2020

U.S. SENATE,
SUBCOMMITTEE ON REGULATORY,
AFFAIRS AND FEDERAL MANAGEMENT,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
*Washington, DC.*

The Committee met, pursuant to notice, at 2:30 p.m., via video conference, Hon. James Lankford, Chairman of the Subcommittee, presiding.

Present: Senators Lankford, Scott, Sinema, Carper, and Rosen.

### OPENING STATEMENT OF SENATOR LANKFORD[1]

Senator LANKFORD. Thanks for joining today. This is the hearing before the Regulatory Affairs and Federal Management (RAFM) Subcommittee, Modernizing Telework: Review of Private Sector Telework Practices During Coronavirus disease (COVID–19). Good afternoon, everyone.

In 1990, Congress passed its first piece of legislation directly related to an employee's ability to be able to work outside of their assigned duty station. The most recent and significant legislation affecting the Federal workforce and teleworking was the Telework Enhancement Act of 2010, which set the current standards for Federal workforce requirements for telework.

With so many changes in the world over the last 10 years, or in the case of just 2020, so many changes, period, this year, it makes sense to be able to take a look at the current telework practices to see what is working, what is not working for the Federal workforce, and to be able to learn the lessons of what is happening in the private sector. We have a responsibility to ensure Federal workforce strategies are relevant, cost-effective, and well thought out.

Even before this pandemic, many private sector companies were giving remote work flexibility to their employees. The Society for Human Resource (HR) Management reported a threefold increase in the number of companies offering remote work options between 1996 and 2016. Obviously, that has accelerated dramatically since then.

The Office of Personnel Management (OPM) reported that in 2018, only 22 percent of the Federal workforce was eligible to

[1] The prepared statement of Senator Lankford appears in the Appendix on page 31.

telework. With the March transition to maximum telework impacting many of these positions not traditionally considered telework-eligible, we need to reevaluate eligibility and how this is determined. Clearly we have more than 22 percent of our Federal workforce that is actually teleworking now.

Since March of this year, both the Federal workforce and many in private industry have been forced into a new, remote, work-centric reality. Almost overnight, Federal agencies and private companies were forced to deal with complex problems like cybersecurity, remote performance management, employee engagement, hiring all these on a very grand scale. The pandemic has been a great disruptor but it also shines a light on broken processes and shows an opportunity for real improvement.

There are some very important telework questions that I believe we need clarity on in order to trudge a clear path forward for the Federal workforce. For example, how do we best prepare employees so that during a future disaster or pandemic we can seamlessly transition to a Federal workforce posture? How do we effectively train managers to stay engaged and to monitor performance of a remote workforce? We want to make sure cybersecurity threats are seriously considered and telework policy conversation are protected.

Being good stewards of American tax dollars, something I talk about often, I believe future cost-savings from reduction in needed office space could be a key component to improving remote work opportunities for Federal employees.

I want to reinvent the wheel, so today we will start a series of Federal workforce-related telework hearings by first reaching out to some individuals in private industry to see what they have learned. Those outside Federal service understand very clearly that creating efficient, cost-savings workforce strategies are less a luxury and more of a necessity.

I want to thank this panel for taking away from their business and their very busy schedules. We really appreciate the opportunity to be able to hear about your views on telework and the lessons that you have learned.

With that I would like to recognize Ranking Member Sinema for her opening remarks.

## OPENING STATEMENT OF SENATOR SINEMA[1]

Senator SINEMA. Thank you, Mr. Chairman, and thank you for holding this very important hearing. I appreciate our witnesses joining us today, and I am particularly grateful to have Mr. John Zanni here. He is the Chief Executive Officer (CEO) of Acronis SCS, a cyber protection and edge data security company based in Scottsdale, Arizona. Also welcome to Mr. Michael Ly. He is an Arizona native who, unfortunately, left our State and now lives in Vermont. I am not quite sure why, but you are welcome back any time.

From the start of the coronavirus pandemic, it was clear that the public and private sectors needed to embrace telework wherever it was possible. It is why I co-sponsored the Emergency Telework Act

[1] The prepared statement of Senator Sinema appears in the Appendix on page 33.

of 2020, to ensure that agencies had the authority to permit maximum telework during the pandemic.

The ability of COVID–19 to spread is scary, and the best way for us to reduce that spread is to follow the Centers for Disease Control (CDC) guidelines, maintain social distance, and wear masks. But most office buildings and traditional workplace setups are not conducive for social distancing. I know many companies in Arizona had to quickly transition their workforces to telework models.

There are inherent challenges to implementing telework. Access to broadband, ensuring security in a virtual environment, providing the appropriate equipment, and supporting employees who feel socially isolated or challenged by the lack of person-to-person contact are some of the hurdles that Arizona companies have had to overcome.

I look forward to discussing these topics with our witnesses so we can develop a better checklist to help both private and public sector entities be more successful with telework.

I also think it is critical that we recognize many jobs cannot be done virtually. Many workers do not have telework options. From first responders to health care professionals, many workers in Arizona and across the Nation put themselves and their families at risk to support their communities. I applaud their efforts and understand that telework is one part of the larger discussion regarding how we keep our communities and families safe.

With that I look forward to hearing from our witnesses and I yield back, Mr. Chairman.

Senator LANKFORD. Thank you. Let me introduce our witnesses for today. Mr. Seán Morris is a member of Deloitte's Government and Public Services (GPS) Executive Committee, and the U.S. firm's Operating Committee. He is Chief Operating Officer (COO) for Deloitte's $4 billion U.S. Government and public services executive business. Mr. Morris has day-to-day operational responsibility for more than 16,000 U.S. and globally deployed personnel. He has responsibility for a comprehensive future of work transformation across HR, information technology (IT), Facilities, Contracts, Finance, Security, Security Compliance, Marketing, and Business Development.

The second person is Lane Wilson, clearly the most important of the four because he is from Oklahoma, so I am glad that you have joined us as well. Mr. Lane Wilson is Senior Vice President and General Counsel (GC) for The Williams Companies based in Tulsa, Oklahoma.

Prior to joining Williams, Mr. Wilson served as a Federal magistrate judge for the Northern District of Oklahoma, and served in private practice for Hall, Estill in Tulsa. Mr. Wilson received his bachelor's degree in electrical engineering from the University of Tulsa, his juris doctorate with honors from University of Tulsa College of Law. Lane, thanks for joining us today.

Mr. Michael Ly is a serial entrepreneur and speaker, cloud accounting professional. He is founder and CEO of Reconciled, a nationally recognized online accounting firm based in Burlington, Vermont. Mr. Ly speaks nationally on the topics of remote work, company culture, entrepreneurship, cloud accounting, and diversity in new leadership.

Prior to Reconciled, Mr. Ly worked for a variety of companies in accounting and consulting roles in Arizona, which has already been mentioned, Washington State, and Vermont. Thank you, Mr. Ly, for being here as well.

Mr. John Zanni serves as the CEO of an American cyber protection edge data security company, exclusively dedicated to meeting the unique needs of the U.S. public sector, including Federal, State, and local government, education, health care, and nonprofit institutions.

Prior to leading Acronis SCS, Mr. Zanni held senior positions at Acronis AIG. Before joining the Acronis family, Mr. Zanni spent 4 years at Parallels and 16 years at Microsoft, a tiny little company in the Northwest.

So I appreciate all of your engagement and for appearing today.

We typically have our witnesses stand and raise their right hand. Since all of you are seated at your desks or tables I assume I will go ahead and have you seated there, but I would like to ask you to raise your right hand because I do need to swear all of our witnesses in, as is the custom of this Committee.

Do you swear that the testimony you will give before this Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. MORRIS. I do.

Mr. WILSON. I do.

Mr. LY. I do.

Mr. ZANNI. I do.

Senator LANKFORD. Let the record reflect both of them answered in the affirmative.

We are using a timing system today. As we go through this process you will see the clock up there. If you are in Grid view they will show a 5-minute countdown for your testimony time. I would like you to be as close as you can to that, to save as much time as we can for as many questions for this. But we are very grateful for both your written testimony that you have already submitted and for your oral testimony as well.

We will recognize Seán Morris first for your testimony.

## TESTIMONY OF SEÁN D. MORRIS,[1] PRINCIPAL, DELOITTE CONSULTING LLP

Mr. MORRIS. Chairman Lankford, Ranking Member Sinema, and Members of the Subcommittee, thank you for the opportunity to testify today on the lessons the Federal Government can learn from the private sector regarding telework. My name is Seán Morris. I am a Principal in Deloitte Consulting's Government and Public Services business, and I have spent my entire life in and around the critical missions of our government, first, growing up in a U.S. military family and professionally for more than 20 years working with government clients. Currently I am the Chief Operating Officer for Deloitte's U.S. Government business, with operational responsibility for more than 16,000 personnel.

I fundamentally believe that challenges pose opportunities to rethink orthodoxies, and so it is my hope that the Federal Govern-

[1] The prepared statement of Mr. Morris appears in the Appendix on page 35.

ment, like Deloitte, can use this challenging moment in history to rethink how and where its workforce performs their important roles for the American people.

Based on the investments Deloitte has made for the past decade in technology, facilities, and our people, for this Subcommittee's consideration I offer four recommendations.

Recommendation one is to continuously invest in IT infrastructure and cybersecurity. Now there are a number of core aspects of this recommendation. For example, consistent investment in the latest cloud-based tools is a game-changer for an organization's ability to rapidly pivot to numerous scenarios, which means IT infrastructure and technology platforms must be a focal point for organizations.

Next, any workforce requires access to reliable broadband to successfully perform their work, which means organizations should provision for different forms of broadband connectivity.

Additionally, critical to operational success in any virtual work environment, the workforce must be equipped with the correct on-the-go hardware and software, which means organizations need to have a secure supply chain to enable the provisioning of IT hardware and software.

And finally, workplaces and supporting IT ecosystems have become more diverse and extended, causing an increase in cyber risks. Therefore, cybersecurity programs require appropriate layers of technical defense. But equally important is the nurturing of a cyber culture where employees understand and counteract ever-evolving threats.

For recommendation two, real estate and location footprint, we are seeing the evolution of location liberation, the concept that the workplace is not limited to any one single physical space. At Deloitte, we are working toward supporting four unique types of workplaces. First, the traditional office is transforming into a community hub where employees come to collaborate. Next, the field is where employees are empowered to be productive, no matter where their work may take them. Then the home, which is where employees can balance work and life while maintaining productivity, and finally, a growing set of third places which include alternative space types.

Recommendation three is centered around performance management. An effective performance management approach is a foundational element for building trust. Deloitte's approach to performance management is grounded in frequent, meaningful conversations. These conversations, when coupled with reliable data, enable us to understand and recognize performance throughout the year. The rapid transition to virtual work presents government organizations with an opportunity to challenge the orthodoxy that physical presence and visibility in the office equals a productive and a high-performing workforce.

Further, shifting to measuring accomplishments and outcomes over activities and labor hours allows organizations to cultivate a work environment of high-performing teams.

And finally, recommendation four, employee engagement. At Deloitte, we invest heavily in an employee's experience, from the recruiting phase all the way through to our alumni program. This full life cycle investment is widely recognized as enabling our ability to attract and retain the most diverse and skilled workforce. To reinforce this point, since the onset of COVID–19, and so as not to lose momentum around employee engagement, we have transitioned many of our learning, social impact, and team-building events to virtual platforms.

In conclusion, the fundamental principle underlying all four of these recommendations is that an organization must consider its human capital to be its core asset, and build its technology and facilities accordingly to achieve a successful work environment.

Thank you again for providing me this opportunity to share Deloitte's perspectives, and I look forward to answering your questions.

Senator LANKFORD. Thank you very much. Lane Wilson.

## TESTIMONY OF T. LANE WILSON,[1] SENIOR VICE PRESIDENT AND GENERAL COUNSEL, THE WILLIAMS COMPANIES, INC.

Mr. WILSON. Good afternoon, Chairman Lankford, Ranking Member Sinema, and distinguished Members of the Committee. I thank you for the opportunity to testify regarding private sector telework policies during the COVID–19 pandemic. I will focus my remarks on how Williams has pivoted and evolved our telework capabilities and policies to maintain operational effectiveness, productivity, and efficiency across our workforce of 4,800 employees in 26 States.

In light of our business, we had to get this issue right. Today we handle about a third of the natural gas in the United States. It is used every day to reliably and affordably heat our homes, cook our food, and generate our electricity. During the COVID–19 pandemic, this reliable source of energy has been crucial to hospitals and the supportive infrastructure they need, and the natural gas liquids we deliver continue to be used as feed stock to make the lightweight materials necessary for much of the equipment and supplies used by those hospitals.

None of this would have been possible without our dedicated employees, who are doing their part during these unstable times, and they are doing it almost entirely by teleworking from field locations and from home.

Williams' success is also due to our commitment to safety, reliability, and responsibility. With this in mind, I will share some key best practices from our transition to 100 percent voluntary work from home in March.

These best practices can generally be categorized into three areas: one, the availability of tried and tested systems and process; two, cybersecurity; and three, technology deployment.

Going into the pandemic, Williams had the advantage of a decade of experience with significant remote work. Williams categorizes its employees as field workers and knowledge workers. Field workers include field technicians, safety specialists, and operations supervisors, and represent 60 percent of our employee talent. Our knowledge workers, representing our remaining employee

[1] The prepared statement of Mr. Wilson appears in the Appendix on page 45.

talent, include our corporate support functions like finance, legal, and human resources.

Though we have central offices in Tulsa, Houston, Pittsburgh, and Salt Lake City, Williams' preference is for our field workers to be in the field, so we have developed processes and tools to enable our field workers to telework. Leveraging these processes and tools allowed us to smoothly transition our knowledge workers to remote work. This underscores the first best practice—a tried and tested system is key for successful telework.

The second best practice is around cybersecurity and the need for multifactored systems as well as employee cybersecurity hygiene training. Because of Williams' critical infrastructure status and commitment to safety, our networking systems already have a layered suite of cybersecurity protection software. Further, our existing infrastructure and protocol allow us to remotely push patches to laptops, so we have continued to protect our devices from vulnerabilities.

With the doubling and tripling of virtual private network (VPN) activity and collaboration software use, we did experience an uptick in malware and phishing, but one that did not impact our business. As a best practice, we increased internal communication to employees with reminders about good cybersecurity hygiene, and made the decision to always have one cybersecurity analyst onsite in case we need to invoke our cybersecurity instant response plan.

Third, regarding technology deployment, our rapid transition to remote work depended on effective collaboration software. We saw the utilization rates of this software increase between 100 and 300 percent for online chats, web calls, and teleconferences. Our transition also relied upon employees taking home their laptops and, in some cases, monitors, headphones, and other assets. Also worth mentioning when transitioning large numbers of employees, it is key to have ample IT support as employees acclimate to the new technology and tools.

Looking forward, we recognize that for some workers telework may continue to be an option, but we are also cognizant of the value of in-person collaboration and idea generation that happens organically in an office environment. Balancing these two factors is important, and while we have not made any final decisions around a long-term telework policy we will continue to track efficiencies and productivity measures to help inform our path forward. We will also capitalize on lessons learned, particularly around employee engagement, and continue to build on these opportunities, even after we are free to return to our office environments.

Thank you again for the opportunity to appear today, and I look forward to your questions.

Senator LANKFORD. Lane, thank you very much. Michael Ly.

## TESTIMONY OF MICHAEL LY,[1] CHIEF EXECUTIVE OFFICER, RECONCILED

Mr. LY. Thank you, Chairman Lankford and Ranking Member Sinema and the Members of the Subcommittee for inviting me to share about Reconciled's approach to telework, or what we at Reconciled refer to as "remote work." My name is Michael Ly and I am founder and CEO of Reconciled. I am joining you remotely from Burlington, Vermont, where I live with my wife and three young children. Vermont is my wife's home State, but I still consider Arizona my home State, Senator Sinema, and visit every year with my family to see my mother and my siblings. I was actually there at the beginning of the pandemic.

Remote work allowed me to continue to run my business, Reconciled. We are an online accounting firm, started about 5 years ago. Today we have about 30 employees, working remotely from 8 States, and serving almost 200 small businesses throughout the country, handling their in-house accounting services, remotely and online. We are recognized nationally in the accounting industry by our innovative approach, and we also speak regularly on the topic of remote work, how to build a strong company culture as a remote work company, and how to keep remote employees engaged.

Since we have been operating as a remote company and completely distributed before it was popular because of COVID–19, our operations have not been greatly impacted as much as our customers.

I want to highlight one primary challenge to remote work that will challenge everyone involved in remote work, and then highlight a few key recommendations. The challenge primarily being children at home, school-aged children at home. This is by far the biggest obstruction to our employees' ability to be productive and successful with remote work. Most of our employees have school-aged children that attend public schools in multiple States. Having children now at home requires us to be very flexible with our employees and their work schedules so that they can both take care of their families' needs, their child's education, as well as their work responsibilities.

In my prepared statement I highlighted six key proposals to remote work success. I want to focus on just a few of those, mainly defining role expectations and outcomes, regular and consistent communication, schedule flexibility, and taking breaks.

Remote workers need to understand what is expected of them to accomplish their jobs successfully. Clearly defining the expectations an organization has for each employee and the outcomes that should result when a job is done well is key for the success of the remote employee. Often employers assume that their workers know what is clearly expected of them. The reality is employees have one expectation communicated to them when they initially start with any organization, but then those expectations change as their organizations change, as their roles change, and when the roles now shift to work from home. So clearly communicating those expectations and outcomes are important.

[1] The prepared statement of Mr. Ly appears in the Appendix on page 50.

The other recommendation is regular and consistent communication. Never underestimate the amount of social interaction that we receive outside of our home in a physical workplace, and imagine you having to recreate those virtually with a remote work team now. Time at the water cooler and spontaneous meetings occur 40 to 60 percent of the time at work, and the rest of your time is done actually doing work, and studies have been done in multiple workplaces across the country. So creating those spontaneous interactions needs to be intentional in a remote work setting, as well as taking regular work meetings, and one-on-one interaction with your supervisors and coworkers also need to take place.

Flexibility is another proposal I have highlighted in my prepared statement. Flexibility may be one of the key benefits of remote work, especially during a pandemic. Flexibility can be seen in multiple ways, including work schedule flexibility, how often employees can take breaks, and from what location a remote employee is allowed to work or can work. The key is articulating a remote work policy that provides standards for the majority of your staff while being broad enough to fit multiple individual scenarios, and that is especially important in light of the fact that school-aged children are now at home.

And then finally, breaks. Taking short and regular breaks throughout the day for remote work employees is the key to their long-term success. Remote employees often find themselves more productive in the short term, but if they do not take regularly scheduled, consistent breaks they find their productivity decreasing and their stamina burning out.

Thank you for letting me come and share, and I am looking forward to helping answer questions.

Senator LANKFORD. Mr. Ly, thank you very much. Mr. Zanni.

## TESTIMONY OF JOHN ZANNI,[1] CHIEF EXECUTIVE OFFICER, ACRONIS SCS

Mr. ZANNI. Chairman Lankford, Ranking Member Sinema, Members of the Committee, it is an honor to join you today. Ranking Member Sinema, thank you for the invitation to come discuss the particular challenges associated with telework. I appreciate the opportunity to share my insight informed by more than 25 years in the cybersecurity field, and a remote worker myself since 2020, including in my current role as CEO of Acronis SCS, an Arizona-based company dedicated to meeting the unique cyber protection needs of the U.S. public sector.

As COVID–19 spread, IT teams had the unenviable job of enabling secure telework capabilities at an incredible breakneck speed. Today's typical home includes a mix of work and personal laptops, smartphones, and network-connected toys and appliances, all sharing access to standard Wi-Fi router with basic security configurations.

With telework, the IT help that we all take for granted in an office are greatly reduced. With increased dependence on applications like Zoom, Teams, and WebEx, that has presented new risks as well people tuning into calls from devices on unsecured networks.

[1] The prepared statement of Mr. Zanni appears in the Appendix on page 56.

However, adhering to a layered “defense in depth” approach to cyber hygiene that adopts relatively simple processes and tools like ours significantly diminishes the dangers of remote work.

As the CEO of a cyber protection company, when this pandemic started I had two priorities. First, ensure the physical and digital safety of my employees. That was paramount. Then continue providing solutions that help our public sector customers stay secure.

On the tech front, we were well-positioned for telework. Similar to how the medical field uses vaccines, diagnosis, medication, surgery, and research to treat illness, we implemented a cyber hygiene plan underpinned by prevention, detection, response, recovery, and post-incident forensics, a framework for digital resilience that I would recommend for any organization.

For Acronis SCS, that plan includes zero-trust architecture, leveraging next-gen firewalls, segmented networks, multi-factor authentication, and certificate-based VPN for access to sensitive resources. This posture helped us shift to telework without fear that an attack on one device would compromise the whole company.

Beyond technical factors, we have taken a holistic approach to ensure the safety and productivity of our workforce. We have reimbursed employees for at-home office equipment purchases, disbursed monthly Internet stipends, and ensured our health insurance supports telemedicine and mental health services. We also host virtual town halls and social hours to keep our more isolated employees engaged, and have flexible schedules for those balancing work with at-home family obligations.

We doubled down our commitment to provide software that meets the U.S. public sector needs, whether keeping mission-critical assets running with our hard and backup software or protecting endpoints with Acronis SCS Cyber Protect Cloud.

While telework has certainly exposed new risks, it has also spurred urgency, and I want to thank the Committee for its work on this front. Chairman Lankford, Ranking Member Sinema, you have been both instrumental in educating the American people on our nation’s cybersecurity vulnerabilities and have developed bipartisan legislation to address them, bills like your Telework for U.S. Innovation Act and the Emergency Telework Act. From this legislation to the cybersecurity-focused NDAA amendments under consideration to the Defense Department’s much-needed Cybersecurity Maturation Model Certification, all signs point to even more urgency across government and a more secure nation and robust economy as a result.

To facilitate public-private collaboration I ask you to consider making the reporting of cyber attacks on Federal, State, and local government agencies mandatory. Similar to testing for COVID–19, if we do not fully understand the scope or the pervasiveness of the problem, we cannot appropriately address it.

Increased telework flexibility is in our nation’s long-term future. America cannot afford to relegate cybersecurity to the back burner. The risks of doing so are simply too high.

Chairman Lankford, Ranking Member Sinema, Members of the Committee, thank you again for the opportunity to be here today, and I look forward to hearing your insights and addressing your questions.

Senator LANKFORD. Thank you very much, and I appreciate your testimony. We will have lots of ways to be able to pick your brain as we go through this as well. I would tell you, on the technology side and the video side, you are taking an exceptional risk, Mr. Zanni, of standing in front of a green screen. I have already imagined how many different ways people could use that green screen and how many places they could put you right now.

Mr. ZANNI. Yes. That is a fair point. But I keep my private life private and watch what I say, but we will see.

Senator LANKFORD. I will defer my questions to the end of our hearing. Senator Sinema has also chosen to do the same thing as well, to be able to defer her questions to the end. So I recognize Senator Carper for his questions now.

## OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you. Thank you, Mr. Chairman. To all of our witnesses, welcome. In fact, you all have some very interesting backgrounds. You have made some significant career changes and moves that one would not have expected, given your early start in life. I am delighted that you are here to share your thoughts with us today.

I am going to start with a question for Mr. Zanni. In your testimony, you state that the modern cyber threat landscape is more sophisticated and relentless than ever before—I would agree—but that many of these threats are not new.

Ransomware is one example of this, as these attacks have continuously posed a threat across different sectors, including State and local government. Educational institutions as well.

More recently, scam emails have been a way bad actors are affecting vulnerable systems. Did you hear that? That sound says we just began our next vote, and maybe our last vote for the day. We will see. It will be over in a second. Maybe. There we go.

More recently, scam emails have been a way bad actors are accessing vulnerable systems while folks are teleworking. How has your organization, Mr. Zanni, handled cybersecurity incidences with employees shifting to telework, and how can Federal, State, and local governments learn from those incidences in identifying our vulnerabilities?

Mr. ZANNI. Thank you. In the context of our company, we took a "defense in depth" approach, which means a layered approach to protection. No single company can provide sufficient protection against ransomware or phishing attacks or other malware. Unfortunately, the weakest link is still humans. We are taught and trained to trust, and that trust is sometimes taken advantage of.

Also, it is impossible for anybody to keep their systems up to date instantly. So by having a multilayer approach in terms of VPN, multi-factor authentication, having a good antivirus software, having good backup and recovery, good anti-ransomware, you really minimize the chances of anything bad happening. And if it does, you can recover quickly, and if you take full advantage of encryption, the likelihood of any data being compromised is very low.

The other part I would like to add here is education. Unfortunately, as a society, we do not understand yet the seriousness of these threats and the tools that the bad actors have. Right? This is not college kids in a dorm room having fun. These are nation-states, well-funded organized crime. They have the same access to machine learning and quantum computing and artificial intelligence (AI) that we have access to. And so without bringing in the experts and the professionals and the tools and the processes to protect ourselves, we just become vulnerable.

And so education and awareness is an absolute key component, and we spend a lot of time, like me here, just educating and driving awareness, so that people really protect themselves and not make security an afterthought.

Senator CARPER. Thank you very much, and thank you for making time to do some of that educating with us, my colleagues and me.

A question, if I could, for Mr. Morris. This deals with coordination with an agency we call Cybersecurity Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS) Mr. Morris, I understand that you are responsible for managing over 16,000 U.S. and globally deployed personnel. Is that right?

Mr. MORRIS. That is correct, sir.

Senator CARPER. Boy. How long have you been in your current leadership position?

Mr. MORRIS. Current role, one year.

Senator CARPER. OK. I read in your testimony that Deloitte practically shared cyber threat intelligence with the U.S. Government agencies, cyber threats before they can cause substantial harm. One of those agencies, I presume, includes the Cybersecurity Infrastructure Security Agency, which is at the Department of Homeland Security. Is that correct?

Mr. MORRIS. Yes, sir. We share it governmentwide and actually within the industry as well. We find it is a good way to collaborate on external threats.

Senator CARPER. OK. Over the years, a number of my colleagues and I worked to give DHS the resources necessary to carry out its cyber mission. We are especially proud of the bipartisanship in Congress that led to the passage of Cybersecurity and Infrastructure Security Act in 2018, 2 years ago.

Could you take a minute and talk a little bit more about your relationship and that of your colleagues with CISA and the other relevant Federal agencies that you work with? Tell us a little bit more, if more needs to be done to improve that relationship between the Federal Government and the private sector in addressing the current threats that we face in light of this pandemic.

Mr. MORRIS. Yes. Thank you for that great question. I will just say that I spent a decade working with the Department of Homeland Security, both pre-9/11 and post-9/11, so it is one of the agencies that I have had a lot of experience with, and it is a fantastic organization.

What I would say is that our cyber professionals work across the Federal Government, State and local governments, higher ed, and in commercial organizations, and we share some of the best practices that we see with all of those organizations, in addition to standard threats that are occurring on an almost real-time basis.

One of the things that I would add about some of the uniqueness of the Federal Government and governments in general is just the multi layers that are associated with our IT systems. And we are noticing a significant amount of success utilizing machine learning, both in our own networks and then sharing that with other government agencies.

The reason that that is a game-changer is the volume that you have to go out and see on a regular basis, and that must be monitored on a regular basis is, quite frankly, too much for a human to do, in any realistic manner, and so machine learning is starting to transform the way that we can interact with all of these layers of network going forward. I think that is a game-changer for agencies, in general, to better utilize.

Senator CARPER. All right. Thanks very much. My time has expired. Thank you all.

Mr. MORRIS. Thank you.

Senator LANKFORD. Stick the landing, Senator Carper. I appreciate that. I am going to ask a couple of questions and then I am going to defer on to Senator Rosen and Senator Sinema, because I will have to run and do a second vote, just like Senator Carper is going to have to do here in just a moment as well. So we will switch back and forth.

But I do want to ask, Mr. Ly, you mentioned about school-aged children and flexibility. Obviously that is a unique issue right now with COVID–19, with schools being closed. I want to ask you, as you are thinking about, let's say, a year from now, are there lessons to be learned? And that is a lot of what we are trying to be able to pick your brain on for all of you, is to pick your brain on what you are doing in the private sector, or things we need to implement in the public sector in the days ahead.

For school-aged children, do you anticipate for telework you will handle schedules differently for teleworkers, not during summertime but during summertime that may be different? Do you anticipate something is going to have to change when we are not in a COVID–19 world but still doing telework?

Mr. LY. Yes. Right now we have been operating pre-COVID–19 world as a remote work and telework company, and so we first set expectations with every employee that the majority of their work, the predominant majority of their work has to be accomplished and done during the normal business hours of 8 a.m. to 5 p.m. Eastern time, which is the time zone we generally operate in, and what our customers generally operate in and want to receive responses from us from.

We also communicate with our employees that they need to be responsive to emails, to communication, to their customers as well as other coworkers that have questions related to work.

I think the really main disruption is the reality of school-aged children at home. Besides that, we have been able to have fairly efficient operations as a business and also set expectations of our employees on their productivity and work outcomes. That work would normally be able to be accomplished during normal work hours, between 8 and 5 p.m. local.

Senator LANKFORD. Right. Before I transition to Senator Rosen here for her questions, what I am really trying to drill down on is do you anticipate, post-COVID–19 lessons learned that you are going to have one type of structure for your telework folks that have school-aged children, let's say January to May, and another type structure that functions during the summer, with those that have school-aged children, or do you just, for your managers you are just basically saying be more merciful to your folks that are managing when they have school-aged children? Do you anticipate there are two different structure or just more mercy and flexibility during the summer?

Mr. LY. I think there is more flexibility during the summer, but as long as you empower your managers and your employees to make decisions that work for their families but also allows them to accomplish their work outcomes and that those are clear for them, then what we find is generally our employees are very flexible with their own lives because they appreciate the flexibility they are being given.

So with the responsibility of being able to work from home, they take that seriously, and they flex their own personal lives to be able to get their jobs done, as well as the needs of their families.

Senator LANKFORD. OK. Fair enough. I want to recognize Senator Rosen for her question time, and then Senator Sinema will follow her directly after that.

## OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you, Chairman Lankford, for waiting for us to come back from votes. I really appreciate it. Thank you, Ranking Member Sinema.

This hearing today, of course it is such an important topic. It is on the minds of every single person I know, whether you are a worker, a business owner. This is one of the many challenges that we have today. So I am so glad we get to come together in a bipartisan way to figure out how we are going to support businesses as employees migrate to some form or fashion of telework, and what kind of flexibilities do we all need to be able to make this happen.

I want to focus a little bit on cybersecurity, and, of course, the pandemic. We have forced many small businesses now to transition their workforce to work remotely, and we know the challenges it faces is sometimes you do not have the right Internet, you cannot get on, the phone signal, whatever those things are. Our companies had very little for planning before having to shift quickly from in-person work to telework.

So, of course, we know there is no shortage of hackers out there. They see this as a prime opportunity to just pounce on, and potentially steal information, get inside someone's place of business. They want to exploit those gaps in security, targeting individuals on secure devices or networks. Many of them are now using things from home that are not secure in the same way their space may have been at the office.

And so, Mr. Zanni, can you talk a little bit about the major cybersecurity challenges that small businesses are facing when they transition? Are the current programs at DHS and Small Business Administration (SBA), do you think they are enough to help us get over kind of this hump of having to figure all of this out? What can we do to help fill the gaps as everyone needs to navigate this?

Mr. ZANNI. So I thank you for the question. Prior to my tenure at Microsoft I was actually a small business owner, a single restaurant, for over a decade, so I have a particular affinity and love for those people who work very hard, day in and day out, to support their families.

The first thing is that, for small businesses, it is still way too complex to figure out how to protect yourself against cyber attacks. Part of that challenge is, of course, with the industry itself, and that includes me. Part of it with the government, providing clear and concise guidance on how to protect yourself. It is not that hard. It is just very confusing today.

We are fortunate. We follow a lot of the government guidelines. But as you know, if you have ever read a National Institute of Standards and Technology (NIST) guideline, they are not two-pagers, right, and it takes some expertise to really go figure that out.

So I think what the government could do better is first awareness and education on how this threat is real. Just like none of us would leave our house with our door unlocked, or even remove the locks and leave, we need to show people that you need to have cybersecurity as top of mind. And even the smallest business is not exempt. In Arizona, a small school district was attacked, a K–12 school. They said, "Why did they attack us? We are nobody." They do not care.

And then the other one is really providing concise guidance, right? It really is just about keeping your system up to date, having the right cyber protection tools, and some people to make that happen. Just like you have made it very easy for me to recycle trash, which I know is more of a physical piece, but it is that same concept, and there is some work we could do together there.

Senator ROSEN. I appreciate that. I appreciate you being a former restaurant owner. I would love to chat with you about that because in Nevada we love our restaurant and hospitality industry, for sure. But I want to thank you for your answer, because 99 percent of businesses in Nevada are actually small businesses. My office, we have heard from hundreds of them. We have connected with every Chamber of Commerce, our small business directors, done over 100 webinars. I have been on many of those with them.

I want to really ask the business owners, the businesses represented on the panel, if you did not turn to the SBA or to NIST or some of those, where did you turn for information to maintain your cybersecurity as you were transitioning? So, Mr. Wilson, I guess we will let you go first, and then Mr. Morris and then Mr. Ly, please.

Mr. WILSON. Thank you, Senator. Yes, I mean, we are not a very small business so fortunately we have a very robust IT department and they were able to transition us in the means that we needed to. So probably not the best one to answer that question for you.

Senator ROSEN. Mr. Morris.

[No response.]

Mr. Ly.

Mr. LY. Right. Because we handle accounting work and we often have access to financial information related to our customers, we, from the beginning, have implemented cybersecurity protocols that are very secure. The weakest link in most remote organizations is what we call "endpoints." Generally they are mobile devices or laptops that are either provided by a company or brought in by an employee themselves. And it is ensuring that the security protocols are set up as well as virus protection, malware protection, and Internet security suites are preloaded onto those devices, as well as ensuring that employees' homes and the networks that they are on are protected and secure, and that they are using VPN software when they are entering into areas that are unsecured, like public Wi-Fi settings, if they are planning to do work from a location that is not their home location.

Also, the more pure cloud-based technology you can leverage, in our opinion, the better, mainly because then documentation or confidential documentation is no longer sitting on those devices but instead sitting in the cloud, in the Internet, and accessed through Internet software, Internet-based software, and that is primarily the practice we have used.

And so we leverage accounting journals, technology journals, and websites that allow us to ensure that we are setting the right security protocols for ourselves and consulting also our clients on the best practices as well.

Senator ROSEN. Thank you. I appreciate that. I know I am just about out of time so I am going to submit this one for the record. But I think about the costs associated with migrating to telework, and I think about the capital investments that can make that may spur our economy. Those are those one-time investments that we are going to do to bring all of our systems up to speed or create that personal protective space we might need, even if people come in or buy laptops, hardware, software, and the like, versus the normal operating expenses. And perhaps Congress can think about how we help you with the one-time capital expense so people's businesses can continue to operate, and that can take it off their daily books, if you will.

So we will look forward to seeing those answers. Thank you, Mr. Chairman.

Senator SINEMA. [Presiding.] Thank you, Senator Rosen.

Hi. It is Senator Sinema again, and my first question is for Mr. Zanni and Mr. Morris. Successful telework is dependent on reliable high-speed Internet and as a member of the Senate Commerce Committee I have repeatedly called for future coronavirus relief legislation to include a long-term plan to invest in broadband infrastructure, ensure we have the appropriate regulatory framework, develop better coverage maps, and utilize Federal resources effectively.

My State, in Arizona, ranks 51st for rural fixed broadband deployment, and three-fifths of rural residents have no access to ground-based broadband. So folks in Arizona frequently tell me the service that exists is often unreliable.

Given that both of you highlighted these types of broadband challenges in your testimony, what advice would you give to other employers seeking to expand telework, those who face similar challenges?

Mr. ZANNI. This is John and I could take the first one, if that is OK.

Senator SINEMA. Great.

Mr. ZANNI. OK. Great. Thank you. So first, I do want to emphasize that we do need to solve the lack of broadband access to rural populations, because that is critical. Today, if you do not have access to broadband in most businesses you are at a competitive disadvantage.

Having said that, there are ways around it until it becomes available. There are products like ours that are optimized for low broadband situations where they are using smaller agents, a lighter footprint, combined solutions to not use as much of the network. Even the teleconferencing software, you will see a very big difference in low broadband situations if you are using Zoom, for example, versus Skype.

And so being able to make sure you identify the tools that work best in those situations, you can still be quite productive. We need to solve the problem of not having broadband access to everybody.

Mr. MORRIS. And this is Seán Morris. Ironically, you may have noticed my picture went away for a moment there, about a minute ago, and actually the power went out in my house, and so it reemphasizes the importance of actually having a backup, which I think is incredibly important. Bad things do happen sometimes, sometimes on a world stage, I guess, as well.

But in any event, what I would say is I completely support John's comments previously. We have to invest in our broadband technology for all aspects of our country, and not just the populated cities but the rural areas as well. We put ourselves at a competitive disadvantage against other European countries, for example, that have made significant investments and are leaps and bounds ahead of us, in many instances, and are better able to take advantage of things like 5G in the future.

Backups are important, at the end of the day, as I proved just a moment ago. From a Federal employee perspective, one of the things that we have done, while it is not perfect, when broadband connectivity is down or not available, in particular, in one of four locations that I referenced in my opening remarks, every one of our employees is issued a smartphone, which enables a hotspot to work and provides some levels of connectivity. It is actually very good. These days it is 4G and moving to 5G.

Senator SINEMA. Thank you so much.

My next question is for first Mr. Ly—I apologize; I think I pronounced your name wrong at the beginning of our hearing—and then also for Mr. Morris. Whether a company is a small startup or a large multinational firm, individual employees are its backbone. Social interaction in the workplace is not only helpful for professional development but also in cementing the relationships inherent in creating a team.

So what steps have you taken to ensure that your employees continue to feel fulfilled and supported while teleworking, and have you discovered any tools available to help employers enhance and maintain that camaraderie amongst the workforce?

Mr. LY. Yes. So thank you, Senator Sinema. The tools we use, we leverage technology to allow for that consist connection to be recreated virtually, that normally happens in an office. It starts on day one, when an employee begins, and starts with their experience with onboarding into a company and their experience with HR. We leverage video technology such as Zoom, and then an internal communication tool such as Slack that replace traditional email but allow instant communication between employees, and allows us to create spontaneous meetings and interactions and collaboration that normally happen within an office.

We also require that every employee has a touchpoint throughout the week with either a supervisor or a coworker, so that they have regularly scheduled times in which they are connecting in with their team virtually. Because again, you are trying to compensate for, as you said, in-person times that happen throughout the day, and we cannot overestimate the amount of social interaction that continues to occur, and the health and well-being that helps with that.

So we are very intentional about that, scheduling that throughout people's calendars, and making that a part of an employee's work responsibility throughout the day and throughout the week.

Mr. MORRIS. I would just add, I agree with those comments. We have invested significantly in what we call the employee experience, throughout the life cycle of an employee's time at Deloitte, and we did not want to lose all of that investment when we went into this full telework environment. And so we have transitioned to almost everything we do for employee experience to a technology and online platform. And what that has allowed us to do is not lose that culture of heavy investment in our employees.

One of the core aspects of our culture is to give back to our communities. We give a significant amount of our time and money to pro bono efforts, as an example, across the country. And we have moved our pro bono activities, our social impact activities to those online platforms that we have, many that are very similar to what was previously shared.

So, at the end of the day the best practice here is do not stop investing in the employee experience. Move it, if you can, to these platforms, and that culture will continue to thrive and adapt.

Senator SINEMA. Thank you. Just a quick follow-up on this topic. Are there specific actions you would recommend a company take regarding telework during a pandemic when feelings of fear and social isolation are often exacerbated?

Mr. MORRIS. Yes. I will just add that, what we did was we encourage our individuals to take time off. That is a challenge that we see at the moment across industries.

The other thing that we did was recognize that well-being is both physical well-being and emotional well-being. And so we gave 80 hours of time off in addition to sick leave and personal time off. So there is a steady focus on that working from home does not equal working all the time.

Senator SINEMA. That is an important point. My next question is a follow-up on kind of building off the question that Senator Lankford asked earlier, for Mr. Zanni and Mr. Morris. I have heard from some Arizona companies that perhaps the chief challenge with teleworking right now is the closure of most of our schools. Parents are managing their children's education needs while also juggling their own work responsibilities. And as we have seen, this requires great flexibility on the part of companies and families.

So what specific recommendations might you have for companies, or for families, on how to set up or expand a telework plan so that people can both manage being a good parent, a home-school teacher, and a good employee?

Mr. MORRIS. John, do you want to start?

Mr. ZANNI. Sure. Yes, that is an incredibly hard problem to solve, especially some of those families live in smaller homes. And it is not just about the child or the dog coming in and interrupting you during a meeting. It is the worrying even when you are in a meeting, are they going to interrupt you? When do I get a break?

The best we can do is first really send the message to these families that as an employer we are here to support them and support flexible work hours, and take the time off that they need. I have one, my head of sales. He came to one day and just said, "John, I need to take 3 days off. I need to give my wife a break so that we do not go crazy." And of course I said, "Immediately."

Longer-term, we have to think about how these workers can somehow segregate themselves or separate themselves enough to not be as distracted or find the right work-life balance. I have seen hotels offering rooms during the day now for telework. I am sure there are other options that will come up. But we need to think together how to do it.

But the first thing is really—I have made sure, for me, one-on-one calls from my head of HR, that everyone in my organization knows family first. If you need a break, take it.

Senator SINEMA. I appreciate that.

Mr. MORRIS. Thank you, Senator. I would just add that the training does start from the top, and that is absolutely a lesson learned that we have had in Deloitte.

The other thing I would say here is that yes, it is families with children. My wife and I are certainly examples of that. Yes, it is very challenging. But it is also other circumstances, and I think it is important to note that in diverse employee networks, that could be an aging parent, that could be a pet that is sick. There are a whole bunch of things that it could equal.

One of the things that we have focused on is this concept of courageous conversation. So very open, authentic conversations with senior leaders in the firm to really get the tone and the culture out there that you can actually ask for time off. It is not looked down upon. In fact, we would like you to share what is going on in your life so that we can adapt our processes and our policies. And we use various communications techniques as well as surveys as a way to get that information and feedback to tailor our programs and our processes.

Senator SINEMA. I appreciate that.

Mr. Chairman, thank you, and I yield back.

Senator LANKFORD. [Presiding.] Thank you.

All right. So going back again to the basic of this whole hearing. We are trying to gather ideas from you, lessons you have learned, so that when we are writing legislation or working through policies for the future for Federal agencies we need to learn what you have done. We will gather, obviously, what they have experienced in the last couple of months and try to apply it to policies.

So let me ask some very basic questions. All of you have been through this in different forms for a while, but this is a very different type of year. I have heard quite a few companies say, "Well, you know what? We are finding good success in teleworking, more so than we thought we would," and then they put this caveat in there, "except when we are hiring new workers."

Because the people existing and teleworking now that you have added so many that are teleworking, they have previous relationships, they are used to collaborating. But when you add a new person or a new group of people into this, trying to learn from each other, figure out how to collaborate, integrating into the culture of your business, that is a very experience when all of their experience has been telework and all the people that physically collaborated now do not know what to do with this new person that is teleworking.

So let me pick your brain on this a little bit. For the long term, are there lessons that we can gain from this on integrating new people into your culture when all of the relationships are telework relationship? Any or all of you can answer that. If you have input for that, we need it.

Mr. LY. Yes, I can start with that, because we hire the majority of our employees in that way, remotely, employees I have never physically met or been present in the same room with.

So it first starts with thinking through your onboarding experience or your employee, your day one experience. And most important for us at Reconciled was what is an employee experiencing in the first day, first week, and first 30 days of being here, and how do we set them up for success? So we leverage technology to do that. We created a dashboard where we literally outline all the different steps of what they are going to experience in those first 30 days, what their different days are going to look like, the training they have to go through online. We require every employee to set up video meetings with others in the company, even if it is not related to their work, just so that they start interacting with other co-workers and other team members in the company.

We also have required meetings with different managers, different leaders in the organization, and they do go through a pretty thorough video orientation with the head of HR as well as their managers, several times that week during the first few days.

So it is important to think through intentionally what is an employee experiencing, what is it like, what are things that they need to see on video, what do they need to see in physical documentation, what can be a quick email, and really trying to create what I call, like in a Disney-like experience. How can you wow them, even in a virtual setting?

And we often have employees say they feel more connected in that experience virtually than they do with most places they have worked physically. So we know the results speak for themselves when we get that feedback from an employee. So it is really that intentional investment, very similar to what you would do to invest in the customer experience, on how do you make a customer feel like they really are connected with you and can trust you. You have to do the same, if not more, with a virtual employee.

Senator LANKFORD. OK. Very helpful. Who else?

Mr. ZANNI. This is John. I will just second what Michael Ly said. It really is about being intentional. We have onboarded a number of employees since COVID. First time in my life I have not met them in person, quite disconcerting at the beginning. But once they start we have a very robust onboarding session. We have teams that keep Zoom sessions on all day, so that people can interact, ensure those video meetings.

I personally will send them a message on Teams to say, "I am right here if you ever need anything." So remove those layers that I am not the fake, inaccessible guy. And it has worked out very well for us.

Senator LANKFORD. OK.

Mr. MORRIS. I will just add one other point. I agree with everything that is being said. We are being very successful in some unusual circumstances here.

But I would add that when we beat this virus and we get to our new normal, my personal perspective is that the need for some level of in-person interaction is important for continuing to cultivate an employee experience and a culture, which is why we think about our workplaces facilities in the four quadrants that I spoke about earlier. It is this dynamic movement across those, where you can have different experiences and different interactions.

Technology is a fantastic game-changer, particularly right now in COVID–19. But I am a believer in some level of human interaction as well.

Senator LANKFORD. So Seán you are saying that you are going to keep those four quadrants even after this, that it is your expectation that you are going to have, if I remember them correctly, collaboration, that you will have home, alternative place, and then there is one other, the field was the fourth one, if I recall correctly. Do you anticipate you are going to still have those four quadrants even after this?

Mr. MORRIS. Yes, Senator, and it is recognizing that an employee may be doing different things at different stages in their careers, so they can move around those quadrants. And that we have taken all those into consideration as we are building the right platforms, and we are building those platforms on that experience, as opposed to the platforms first.

Senator LANKFORD. All right. Lane, where are you as far as trying to be able to onboard people during this time period? Any lessons that you have learned that could help us in the Federal workforce?

Mr. WILSON. Yes. We are onboarding people as we speak. I think this boils down to leadership, frankly, and intentional touchpoints.

So I lead a team that even before the pandemic was not on the same floor as I am here in Tulsa, and the majority of the team was not even in Tulsa. They were spread across four different States. And being very intentional about getting them in front of leadership, through town halls, for example. We are now doing monthly town halls as opposed to before we were doing quarterly town halls. Making sure that they get a feel of the culture from the leadership, and then as a leader, making sure that you are having those intentional interactions with your team, and also making sure that your team members are having intentional interactions with themselves. And then you cascade that down through your organization.

We probably have five, six layers here at Williams. So we have to make sure that our supervisors, who might be managing a team of eight or nine people, either out in the field or in an office, are doing the same thing, that they are talking to and visiting with and having collaboration sessions with their teams, and also making sure that their team members are doing that. And when you bring somebody new on board, that is even more critical, that you build in an expectation that, hey, you have a new team member. Have you reached out to them? Have you had a videoconference with them? Have you talked to them? Do you know anything about them? Have you gotten to know them in any way?

And so I think it is really just about very intentional leadership.

Senator LANKFORD. So let me delve in on this a little bit more, for all four of you, if any of you want to be able to answer this. Has your perspective changed, or maybe it has not? I am interested to be able to know what that might look like, that there are certain positions that you will no longer hire those within a geographic area, or certain tasks and certain jobs you know that they are very capable of teleworking from anywhere in the world, for that mindset, but at least anywhere in the country. Is there a perspective that you have that in the future there will be certain jobs that you will hire remotely, find the best person no matter where they live, and have them permanently work not in an office space?

Mr. LY. Yes. I can speak for the accounting industry. My peers who were not previously doing telework or remote work, and believed that was impossible and saw what we did, said, “I am not sure how that is possible. I have been forced to.” And they are finding a lot more efficiency, a lot more productivity when they implement the best practices around it.

Senator, I was watching a YouTube video of yours on YouTube. I was really inspired by this daily interaction or weekly interaction you have with different people from your home State that visit D.C., and you have coffee with them. I was thinking to myself, wow, imagine being able to have that kind of coffee virtually with people all over the world that are from your home State, and be able to answer questions and connect with them, both formally and informally.

And that is what we do also—that is what I recommend also for most companies who go to remote work, is an example is we have a daily virtual lunchroom. Anyone can jump into that virtual lunchroom. Everyone has lunch, or has a meal. And so they can go in and interact with one another and not even talk about work, or we do the same thing with coffees with the CEO. I have a weekly coffee where any employees can jump in and have an informal time with me.

As Lane said, all those interactions take leadership, it takes modeling, and brings kind of that aspect of the culture that you are trying to build that normally happens in an office.

But there are definitely roles we are hearing from clients as well as from peers in the accounting industry, which is very slow to move in regards to technology, that are surprised at how well it is working, and how now they are expanding the different locations they are willing to hire from.

Senator LANKFORD. OK. That is helpful. Let me ask about merit-based affirmation. Some of that is remote working. It is harder to be able to stop by their cubicle or stop by their office, compliment them on the work that they are doing. That has to be a very intentional thing for a leader to manager to be able to do in that situation. It is also, when we talk about raises, when you talk about promotions, it is difficult to be able to do when you are not interacting with that person, when you are literally getting data about that person's performance rather than interacting with them, to be able to know what they are doing.

How are you handling merit-based affirmation, whether that be promotions, raises, whatever that may be?

Mr. WILSON. Senator, this is Lane again. It is sort of much of the same. I insist that all of my performance reviews and all of the performance reviews of my team, if the person is not there in your office, and obviously they are not now, that has to be done by videoconference. It has to be done face to face. You need that interaction, and I think even after this pandemic is over, if you have people that are working remotely, as Seán said, I think you have to get them all in together, on an occasion, and it is obviously better to have those discussions in person. But if you cannot, adding the face on the video is a big benefit.

Senator LANKFORD. Yes. Are you adding some sort of metrics that you are trying to track performance with, or how are you handling that? Is there a piece of software that has been useful to you, to be able to evaluate the performance or quotas, whatever it is that you are putting on individuals in the field, to be able to know customer service responses? How do you manage that?

Mr. WILSON. Yes. So we have used that sort of collaborative software for a very long time, in terms of our sales representatives, the people in the field who are supposed to be interacting with customers. From a high level, in the office environment, with, lawyers, HR professionals, accountants, that sort of thing, we do not get down to the individual level. There may be some privacy issues you have to think about there. But we do track that on a very broad level. As I indicated in my testimony, we have been able to get a pretty good handle on the fact that our employees are utilizing this collaborative—the teleconferences, the chatting, that sort of thing—on a much higher rate than they were before. And that gives us some comfort that these interactions are occurring.

Senator LANKFORD. OK. Other input from other individuals?

Mr. ZANNI. This is John. I can add that my experience has been that employees really like having ownership, and measurable goals, right, because it sets expectations appropriately. In most cases when you cannot assess whether people are doing their job are not, part of the problem, or even in some case most of the problem, it is the manager themselves who have not really thought what they want them to do and how to measure it. It is hard, but once you do that, then these questions of, "I have not heard from James Lankford in 2 days. I wonder if he is actually working," they come up very rarely because you just look at the results or the output.

And so that is what we have focused on and it has been pretty effective.

Senator LANKFORD. Good. By the way, I know James. He is working.

Mr. ZANNI. OK. Good.

Senator LANKFORD. Anyone else?

Mr. MORRIS. Senator, I would just add, and I referenced this in my opening remarks, that designing a performance management system that is built around regular interactions between a supervisor and an employee is a builder of trust, at the end of the day. I think setting goals and reevaluating those goals through that system, where you are having regular conversations and using data around it, is incredibly important.

What I would also say is making sure that those goals are balanced. We like to think of them in not just quantitative terms, which is where it is easy to count, but also in qualitative. And concepts like leadership and agility, and looking at aspects of 360-degree feedback. All of these are important aspects to build that trust between a supervisor and an employee, in a sort of modern performance management approach.

Senator LANKFORD. OK. Let me ask this. Several of you, in your written testimony or in your oral testimony, talked about increasing need for IT professionals, cybersecurity. John, you mentioned specifically the challenge of people working from a home system that you have no idea how that router was actually set up, the security settings that are there. They are working in unsecured networks at a coffee shop at some point. There are a lot of cyber challenges there.

Are there any lessons learned that we should be aware of on the Federal side that we could implement?

Mr. ZANNI. I will start. Absolutely. So I am glad you brought this up, because one of the biggest challenges is there is a lack of cybersecurity experts within the country. Today there are over 600,000 open positions, about 50 percent more than before COVID. And without the people—you have people, processes, and product—without the people you will not be able to implement a good, secure solution.

And so where the Federal Government could help is getting those people trained. For example, one of the—I still believe in this, but I actually created a charitable foundation called Acronis SCS Vets, specifically focused at taking our U.S. veterans and military spouses, getting them the nationally recognized certificates they need to get self-sustaining jobs in cyber. So it is a reskilling effort.

It has been very successful. Unfortunately, my numbers are nowhere near to where they need to be to impact 600,000 people. This is an area where I think the government can help a lot in providing cyber training to individuals who need to be reskilled, or are willing to learn them, to go work for all these businesses.

Senator LANKFORD. OK. Other input from others? Michael, I think you mentioned this as well in your statement.

Mr. LY. Yes. I think the one thing is, as much as you control the endpoints—the laptops, the mobile device that your employees are using—I would be hesitant to allow too many of your employees to bring their own devices, because you have less control, unless you make them basically sign the device over to your company or over to your organization. So as much as you can basically protect, secure the endpoints, as well as their home networks, is important.

And then monitor and make it really clear that employees need to let you know when they are traveling or when they are planning to work at a different location other than their home network, because that is where also cybersecurity threats and accidents happen, where they are in a public Wi-Fi setting, they are in the airport working, they are in a coffee shop working, and those networks are not secure, and they forget to turn on their VPN, like required.

So just making sure that you have technology that alerts you when employees are in different Internet Protocol (IP) settings or locations that are unsecure, and making it really clear that there are strict standards that your company is going to abide by, as people work and do remote work, and you want them to do it securely and correctly.

And then who, also, they give access to their devices to. So often you give them a laptop and then they allow their kids, or maybe they allow a partner or a family member to use it for web browsing or gaming. You want to make it really clear that those devices are for work, and that any other kinds of software or activities should be prohibited so that it reduces the amount of cybersecurity threats, even for a small business.

Senator LANKFORD. So is there lockdown software, anything that you have that prohibits someone from getting online without using the VPN, or does not allow them to be able to download applications without having an administrator log in, or setting that you have created on that? I am still interested in if they have a company laptop but they are on a home Wi-Fi system. Their router may be 4 years old and unsecured. Do you require that the company also installs their router at home?

Mr. LY. Yes. So you want to make sure that you provide, one, a stipend to cover the costs for all those things, or you, yourself, as a company, cover those costs, and two, ensure that those are installed correctly, with password protection that is secure, as well as that the laptops themselves have updated virus protection on a regular basis. And there is software that we use to be able to do that to the computers that we have given to our staff.

Senator LANKFORD. OK.

Mr. WILSON. Yes, Chairman Lankford, a couple of things. So when I was with the Judiciary, I do not know if it is worth visiting with them or not, but we were already unable to add software to the laptops that we were provided by the Judiciary. We here at Williams have VPN always on, so there is no choice. If you are on a wireless network you are VPN'd into the network.

Then finally I would just say record Michael's last answer, transcribe it, and get it out to every Federal employee who is working at home.

Senator LANKFORD. OK. We will see if we can actually get that done. That is very good advice. That is why we are gathering things at this point.

Let me ask a question about personally identifiable information (PII). All of you are in businesses that you are dealing with some information that individuals obviously, some more than others, in accounting and background and such.

I will give you an example. The State Department, earlier this year, in March, April, May, June, just stopped doing passports at all. They had no system in place that if someone needed a passport, their passport expired, whatever it may be, they just could not get it because there was no structure in place with the State Department to be able to handle that kind of document in a remote setting. And so the alternative was just stop doing it. We had about 1.7 million passport requests just back up immediately.

Obviously, State Department is reevaluating that at this point, trying to be able to figure out how to do that. Multiple other entities, whether it be the Internal Revenue Service (IRS), everyone else, multiple agencies in the Federal Government deal with very private or proprietary information through processes.

Anything that you would say, in particular, dealing with documents, dealing with items that are personally identifiable information, that you would teach the Federal Government to say, "Here is something to know about this and how to be able to protect that information," even if someone is working remotely? Or would you say there is just no way to be able to do it current technology, we just cannot handle it?

Mr. ZANNI. Well, I will start. I have learned in software you can never say that you can do everything perfectly, but there are ways to mitigate the risk. First, the Federal Government has a great standard called Federal Information Processing Standards (FIPS) 140–2—there is a 140–3 coming out here shortly—which is about how to use encryption, both at rest and in transport, to protect data. We have FIPS-certified product. At my company I bought FIPS-certified routers from Palo Alto Networks.

So first just implementing those standards will radically reduce the risk that personally identified information leaks. And that, to me, is straightforward.

The other thing is segmenting networks and using that zero trust model, where you control who has access to that information. I am the CEO of the company. If you are one of my customers, I cannot get that information, because I do not need it on a day-to-day basis. If I want it I have to actually go make a request. So somebody can take these images and my voice and pretend they are me, but they still will not have access, because I just do not have access.

So there are a number of things you can do that reduce the risk to almost zero.

Senator LANKFORD. Other input?

OK. Let me move on to another question then on this. There is a lot of conversation about telework that is in the efficiency standard, and most often it goes toward physical footprint, leased space, your owned space in a headquarters building at some point.

There are some people who will make their decision based on a footprint space and what costs, just depending on the cost of real estate in a particular area. In Washington, D.C., obviously, real estate is exceptionally high. But if you get into Oklahoma City and Tulsa, and other places around the country, it is not a high cost. And so companies will make different decisions based on telework.

My question to you is, more than just physical space leasing or keeping that space open and paying the utility bills for it, are there other areas of efficiency that you look at to be able to decide if I am going to have a particular person teleworking, they are more efficient, they work better in a home setting or in a third location, if I can say it that way, at some point than they would in an office setting where they are just as efficient, if that, and so we find other efficiencies or reasons to be able to have someone telework?

Mr. LY. Yes. I can answer this one. Before the pandemic, and still even now, unemployment in the accounting industry was very low. It was lower than the historic unemployment of the country, so it was lower than that. And so one advantage to telework—and we actually did not decide telework regarding footprint—we chose it because we wanted to access the talent nationwide. We wanted to be able to combat against the lowest unemployment rate that we were seeing historically in accounting and finance.

And we were able to access a workforce that traditionally cannot go into physical office, and that is stay-at-home moms. So these are moms that need to be available for their school-aged children, they are doing drop-offs and pickups, they have a 4-to 6-hour window during the day, and then they might have some flex time in the evenings or weekends to do the rest of their 40-hour week.

That allowed us to access a workforce that normally would not show up on unemployment rolls or not looking actively for work, traditionally in the accounting field. And so that is why the majority of our workforce actually is made up of stay-at-home moms and dads who want an alternative to the traditional workplace.

So I would say for sectors that are looking for access to larger—access to more, nontraditional workers or access to workers that would not normally apply for your job, this is a huge advantage for us in the private sector.

Senator LANKFORD. OK. So what I have learned so far from the hearing today is we desperately need accountants and we desperately need IT folks around the country. So if anyone is 21 years old and listening, we have two good career fields for you right now.

Other ideas or other thoughts about efficiencies or reason to do teleworking?

Mr. MORRIS. Senator, I would just add that I think challenging ourselves to re-architect the job type in the first place is an important thing to think about. So, for example, thinking about a crowd-based model to solving particular challenges that an organization has, as opposed to one individual working for 40 hours a week in a more traditional setting, I think could have significant efficiencies.

Somebody referenced earlier the State Department and the U.S. military, and if you look at crowds associated with those two organizations, think about spouses in those two organizations, those are usually underemployed individuals that have a lot to offer, that could provide significant efficiencies to the U.S. Government, using a different talent model.

Senator LANKFORD. OK.

Mr. ZANNI. I would also add that the younger generation—well, my generation, or at least me, think of telework, up until COVID, as a privilege, not a right. The younger generation just expect it, right? I am always connected. I should be able to work wherever I am. So security concerns aside, similar to Seán, if you want access to the best talent and the fullest employee pool, you are going to have to enable telework.

Senator LANKFORD. OK. Lane, I want to ask you one more quick question and then I am going to try to wrap this hearing up and get final input from everyone. Lane, you have to deal in the field with issues of rural connectivity. I know we have already spoken about broadband before, but other solutions and options that you have seen or that have been explored, whether it be satellite Internet, whether it be phone hotspots and other things? Is there anything else that you want to be able to contribute in dealing with areas where it is more difficult to be able to get access?

Mr. WILSON. Yes. I think you kind of hit the nail on the head, and somebody else mentioned earlier the hotspots. So when we have somebody in the field that cannot get good broadband access—and there is no doubt, in rural areas, in Oklahoma and really anywhere in the country, the broadband access is not as good, it is not as robust as it is in more urban areas—the hotspots are the best solution that we have found.

A not-so-optimal solution is just not use the video, but obviously we would prefer to be able to use that. But I think that is the best solution right now, until we get the better broadband service into rural areas.

Senator LANKFORD. Yes. Let me try to wrap this up if I can. Any input that anyone has—let me open this up to a very open-ended question—any input from anyone, that you want to make sure that you recommend to the Federal workforce, regardless of what agency it is, when they are thinking about telework, to consider this in the process, to be able to make sure we get it on the record?

Mr. LY. The only final thought I had was because this is fairly new to many Federal agencies to think about this as small teams. So, from large organizations to small companies, everyone can look at their workforce as a make-up of small teams, with managers, supervisors, and a small set of employees. If you are able to apply these practices in small teams then it makes the idea or the hill to climb a lot smaller, and it seems a lot more doable. So think of small teams of half a dozen or less, where there is a supervisor or a leader in their small team and you are practicing remote work proposals that we have all stated, and the security protocols needed in that. It allows for better communication, better accountability, and quicker response time, as well as agility to move, if you need to make changes during the pandemic.

Senator LANKFORD. OK. Good input. Anyone else?

Mr. MORRIS. I would add just one thing, and that is that human-centered design is so important when we are thinking about adapting policies, changing processes and different technologies. So really putting the lens on the human as we start to think through these changes is a best practice.

Senator LANKFORD. OK. That is helpful.

Mr. ZANNI. And this is John. I would add, as a Federal Government, thinking about some standards or best practices around telework and securing telework. You have heard a lot of great antidotes here, but there are a lot of small businesses, especially, and other agencies, remote cities, that could use that guidance in a way that is easy for them to consume.

Senator LANKFORD. OK. Thank you. Lane, any final comments?

Mr. WILSON. Yes. I mean, look, it is just so easy to fall prey to out of sight, out of mind. And I think our biggest challenge, especially in a workforce the size of the Federal Government's workforce, you have to get your leaders to understand that as we move to more of a teleworking environment they have to keep up those touchpoints. I know a lot of people have said that today, but that cannot be overstated.

Senator LANKFORD. Does your management structure have to be smaller, Lane, at that point? Do you have fewer people that you are managing through telework, or does the same ratio still work?

Mr. WILSON. Yes. I really have not found that to be the case. I mean, you gain some efficiencies, like not commuting back and forth. You pick up some time here and there. People are more motivated oftentimes when they work from home. Some people are not. But we have not found that we have had to reduce those ratios, as long as our managers and supervisors and leaders are being efficient and proactive.

Senator LANKFORD. Yes. Quite a few people that I have talked to have said they have increased their efficiencies dramatically in their workforce because they do not have the travel time, they do not have other social distractions at work. They were able to just plan their day a little bit differently, and, quite frankly, get up, get going. They have more time to be able to read the paper, catch up on news, catch up with their family, and not commute, and then start on time and take off. And less stress, depending on the city that you live in and what your commute is normally like back and forth. That is a pretty significant change for them.

Plus it is really nice for parents of small children. They are wonderful distractions but you also get a chance to see some things that you would have missed just in life with them. So there are some built-in rewards there as well, with the little ones that are running around.

Any final comments from anyone? Otherwise I want to be able to wrap up and I want to make sure I get anything else on the record that we need on the record.

Mr. WILSON. Thank you for your time. Thanks for having us.

Mr. ZANNI. Thank you.

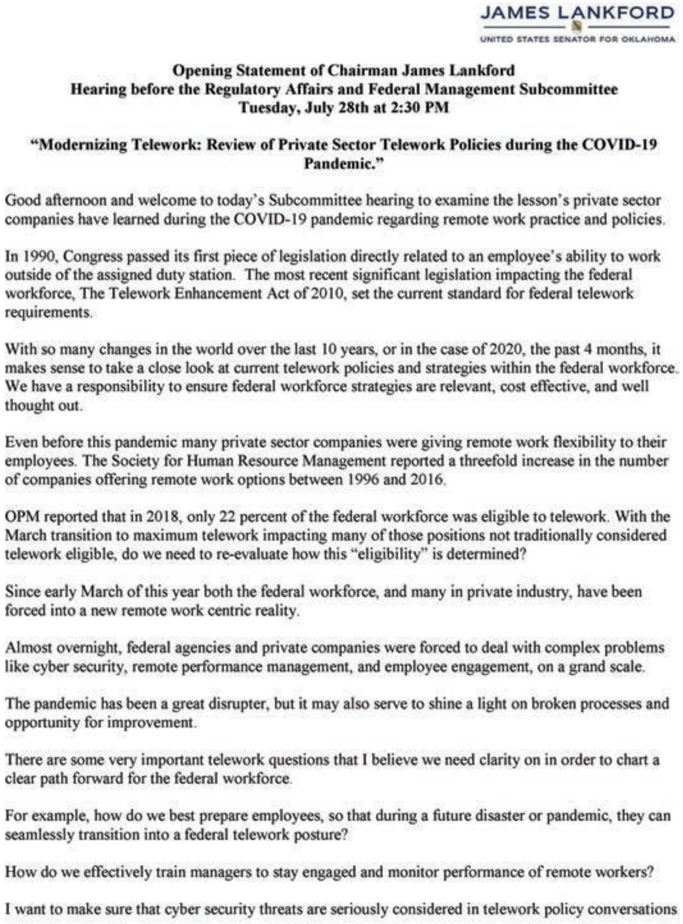
Senator LANKFORD. Gentlemen, thank you very much. I very much appreciate, as I mentioned before, your written testimonies—a lot of time went into that—as well as your oral testimony. I want to tell you that the invitation is open if you have additional input to be able to give to our team as we are trying to be able to pull together ideas and policy changes for the Federal workforce. The last time this was done was 10 years ago. Obviously there are a lot of lessons that have been learned, and we want to make sure we capitalize on those lessons, and to be able to implement those as fast as we can across the Federal workforce in the days ahead.

So that does conclude today's hearing. The hearing record will remain open for 15 days until the close of business on August 12th for submissions, statements, questions on the record, whatever individuals may want to be able to add to the record as a whole.

So with that the hearing is concluded, and I thank all of you again very much.

[Whereupon, at 4:06 p.m., the Subcommittee was adjourned.]

# A P P E N D I X



JAMES LANKFORD
UNITED STATES SENATOR FOR OKLAHOMA

**Opening Statement of Chairman James Lankford**
**Hearing before the Regulatory Affairs and Federal Management Subcommittee**
**Tuesday, July 28th at 2:30 PM**

**"Modernizing Telework: Review of Private Sector Telework Policies during the COVID-19 Pandemic."**

Good afternoon and welcome to today's Subcommittee hearing to examine the lesson's private sector companies have learned during the COVID-19 pandemic regarding remote work practice and policies.

In 1990, Congress passed its first piece of legislation directly related to an employee's ability to work outside of the assigned duty station. The most recent significant legislation impacting the federal workforce, The Telework Enhancement Act of 2010, set the current standard for federal telework requirements.

With so many changes in the world over the last 10 years, or in the case of 2020, the past 4 months, it makes sense to take a close look at current telework policies and strategies within the federal workforce. We have a responsibility to ensure federal workforce strategies are relevant, cost effective, and well thought out.

Even before this pandemic many private sector companies were giving remote work flexibility to their employees. The Society for Human Resource Management reported a threefold increase in the number of companies offering remote work options between 1996 and 2016.

OPM reported that in 2018, only 22 percent of the federal workforce was eligible to telework. With the March transition to maximum telework impacting many of those positions not traditionally considered telework eligible, do we need to re-evaluate how this "eligibility" is determined?

Since early March of this year both the federal workforce, and many in private industry, have been forced into a new remote work centric reality.

Almost overnight, federal agencies and private companies were forced to deal with complex problems like cyber security, remote performance management, and employee engagement, on a grand scale.

The pandemic has been a great disrupter, but it may also serve to shine a light on broken processes and opportunity for improvement.

There are some very important telework questions that I believe we need clarity on in order to chart a clear path forward for the federal workforce.

For example, how do we best prepare employees, so that during a future disaster or pandemic, they can seamlessly transition into a federal telework posture?

How do we effectively train managers to stay engaged and monitor performance of remote workers?

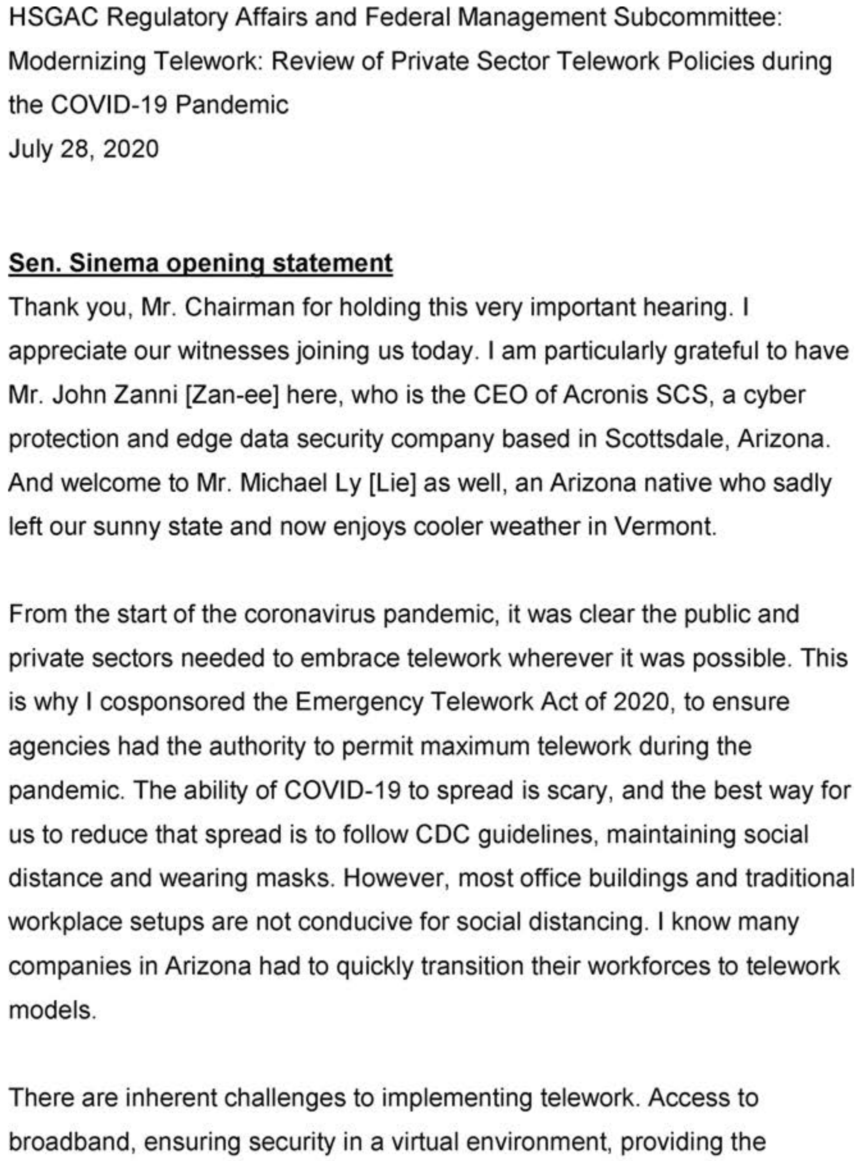
I want to make sure that cyber security threats are seriously considered in telework policy conversations

Being good stewards of American tax dollars is something I talk about often. I believe future cost savings from a reduction in needed office space, could be a key component to improving remote work opportunities for federal employees.

We don't want to reinvent the wheel, so today we want to start a series of federal workforce related telework hearings by first reaching out to our friends in private industry. Those outside federal service understand very clearly that creating efficient cost saving workforce strategies, are less luxury, and more necessity.

I want to thank this panel for taking time away from their businesses and very busy schedules. We really appreciate the opportunity to be able to hear about your views on telework and what lessons you have learned.

With that, I would like to recognize Ranking Member Sinema for her opening remarks.



HSGAC Regulatory Affairs and Federal Management Subcommittee:
Modernizing Telework: Review of Private Sector Telework Policies during the COVID-19 Pandemic
July 28, 2020

**Sen. Sinema opening statement**

Thank you, Mr. Chairman for holding this very important hearing. I appreciate our witnesses joining us today. I am particularly grateful to have Mr. John Zanni [Zan-ee] here, who is the CEO of Acronis SCS, a cyber protection and edge data security company based in Scottsdale, Arizona. And welcome to Mr. Michael Ly [Lie] as well, an Arizona native who sadly left our sunny state and now enjoys cooler weather in Vermont.

From the start of the coronavirus pandemic, it was clear the public and private sectors needed to embrace telework wherever it was possible. This is why I cosponsored the Emergency Telework Act of 2020, to ensure agencies had the authority to permit maximum telework during the pandemic. The ability of COVID-19 to spread is scary, and the best way for us to reduce that spread is to follow CDC guidelines, maintaining social distance and wearing masks. However, most office buildings and traditional workplace setups are not conducive for social distancing. I know many companies in Arizona had to quickly transition their workforces to telework models.

There are inherent challenges to implementing telework. Access to broadband, ensuring security in a virtual environment, providing the appropriate equipment, and supporting employees who feel socially isolated or challenged by the lack of person-to-person contact are some of the hurdles Arizona companies have had to overcome.

I look forward to discussing these topics with our witnesses so we can develop a better checklist to help both private and public sector entities be more successful with telework.

I also think it is critical that we recognize many jobs cannot be done virtually. Many workers don’t have telework options. From first responders to healthcare professionals, many workers in Arizona, and across the nation, put themselves and their families at risk to support their communities. I applaud their efforts, and understand that telework is one part of the larger discussion regarding how we keep our communities and families safe.

With that, I look forward to hearing from our witnesses.

# Written Testimony of Sean Morris
# Principal, Deloitte Consulting LLP
# Before
# Senate Homeland Security and Government Affairs Committee
# July 28, 2020

## COVID-19 and the Virtualization of Work: Responding, Recovering, and Preparing to Thrive in the Future.

## INTRODUCTION

Chairman Lankford, Ranking Member Sinema, and members of the Subcommittee: thank you for the opportunity to testify today on the lessons the Federal government can learn from the private sector regarding the future of virtual work. I appreciate the Subcommittee's attention to this matter and recognize how important this is to each of you, your colleagues, and your constituents. I am honored to share with you Deloitte's strategy and approach to virtualizing our workforce and our related response to COVID-19. This pandemic is an unprecedented challenge affecting us all. My experience is that challenges pose opportunities to rethink deep-rooted orthodoxies and so it is my hope that the Federal government, like Deloitte, can use this moment in our history to rethink how and where its workforce performs their important roles for the American people. Further, now perhaps more than ever, this is as an opportunity to accelerate the Federal government's ability to access, engage and retain top talent in support of its critical missions as we recover and rebuild from this unprecedented crisis.

My name is Sean Morris, and I am a Principal in Deloitte Consulting's Government and Public Services Practice (GPS). I have spent my entire life in and around the critical missions of our government, firstly as a military family member to a 26-year veteran of the United States Air Force and professionally for more than 20 years, dedicating my career to helping Federal government clients. Currently, I am the Chief Operating Officer (COO) for Deloitte's $5 billion US Government and Public Services business and have day-to-day operational responsibility for more than 16,000 US and globally deployed personnel. In this role, I sit on the firm's Operating Committee, overseeing a comprehensive future-forward transformation for Deloitte's GPS business across all aspects of HR, IT, Facilities, Contracts, Finance, Security, Compliance, Marketing, and Business Development. This transformation is strengthening Deloitte's operations in response to the rapidly evolving demands of our **work, workforce, and workplaces.** These are the three dimensions of the future of work, which we have anticipated for years, but are quickly being made more critical and relevant for us all during the COVID-19 pandemic.

## OUR APPROACH

All organizations have been impacted by COVID-19. The private sector is responding to many of the same challenges that the government is faced with: ensuring the safety of its workforce while fulfilling its critical missions. Today, I will share my perspective on how Deloitte is responding to these challenges – what we did and why, and what we have learned as a result.

Deloitte's workforce model is designed to be adaptable to a "work from anywhere" environment. Due to the nature of our work, across offices, client sites, and travel in between, we were technologically and culturally primed for a quick transition to almost fully virtual work once COVID-19 necessitated the closure of our office locations and client sites. One of the biggest advantages of this approach is that we are less constrained by geographic boundaries for talent. However, we also knew that we needed to be strategic about this transition – like our government clients, some of our mission-critical work needed to occur in secure locations. Our teams also had to adjust to virtual onboarding and collaboration at a pace and scale we had not planned for. Additionally, we knew that our employees faced unprecedented levels of stress in finding their new "work-life balance" as disruptions to schools and general day-to-day activities resulted in increasing care levels for family members and loved ones.

I am pleased to report, thanks to a dedicated team effort, our response to the challenges posed by COVID-19 was strong – no downward trends in client satisfaction, productivity, or employee morale. I fully believe this is because we used a **strategic approach to determine the best ways to get our work done** in a constantly changing and highly unpredictable environment, and because above all else, we **made decisions that put our employees, and their wellbeing, first**.

Our approach to virtual work in the era of COVID-19 anticipates that we will likely not return to the way we worked previously. The world of work is, and has been, fundamentally changing, and COVID-19 is an accelerator of that change. As we advise our clients, organizations that attempt to just "return to the office" are missing the opportunity to take advantage of the positive changes a new normal can offer. As depicted below in *Figure 1: Designing a Roadmap to the "New Normal,"* the three phases of **Respond, Recover, and Thrive** maps the immediate short-term need to support employees through the COVID-19 crisis, the subsequent imperative to build a flexible and future-forward strategic plan for recovery, and the ultimate opportunity to thrive and embrace the future of work.

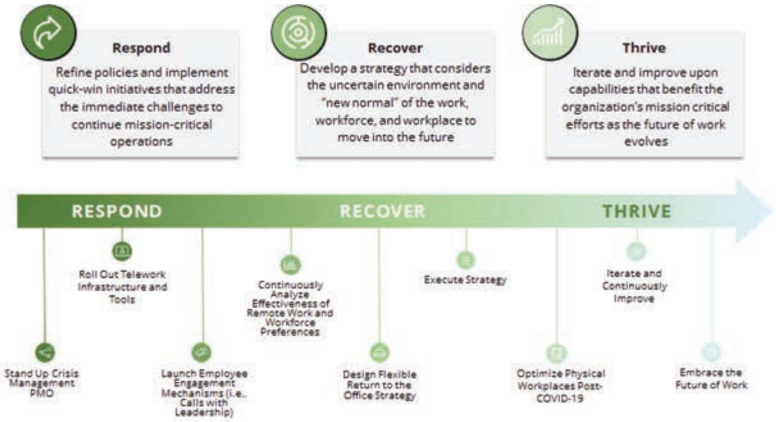

Respond
Refine policies and implement quick-win initiatives that address the immediate challenges to continue mission-critical operations
Recover
Develop a strategy that considers the uncertain environment and "new normal" of the work, workforce, and workplace to move into the future
Thrive
Iterate and improve upon capabilities that benefit the organization's mission critical efforts as the future of work evolves
RESPOND
RECOVER
THRIVE
Roll Out Telework Infrastructure and Tools
Continuously Analyze Effectiveness of Remote Work and Workforce Preferences
Execute Strategy
Iterate and Continuously Improve
Stand Up Crisis Management PMO
Launch Employee Engagement Mechanisms (i.e., Calls with Leadership)
Design Flexible Return to the Office Strategy
Optimize Physical Workplaces Post-COVID-19
Embrace the Future of Work

*Figure 1: Designing a Roadmap to the "New Normal"*

**Respond**: Immediately, we had to harden our virtual work capabilities by engaging strategic communications, crisis management, operations, technology, and infrastructure. We rapidly stood up a Program Management Office (PMO) to centrally coordinate this effort, and our national leaders began hosting weekly calls with their respective businesses to share relevant health information about the pandemic and its impact on how we were responding and working with clients. In short, we increased the regularity of communications, across our leadership teams and with our employees, and adopted an 'answer virtually any question' approach. Most importantly, we prioritized decision frameworks with the safety and voice of our employees at the center of everything we chose to do.

**Recover**: For us, and for many of our clients, this phase is the most critical and can also be the most challenging. We are deliberately analyzing and rearchitecting how work gets done – whether certain activities or roles can be permanently virtual, or a blend of both virtual and onsite. Specifically, this phase is more than just enabling an option and making it productive and fulfilling – it's also about deciding what options are best for the types of work that need to be done. This is how we guide our clients to design their recovery strategies towards the post-COVID "new normal."

In Deloitte's case, we know that the landscape of our workplace is changing. We are not bringing everyone back to the office anytime soon, and in fact, we have identified that some work will remain virtual – the COVID-19 experience has shown us that work is just as effectively done virtually as it was in person. We, however, advise against making these decisions without a strategic approach that considers each of the three dimensions of the work, workforce, and workplace:

- We seek to **understand and prioritize the work** that is being done. We ask questions like: What work is mission-critical and impossible to do virtually? What work has successfully transitioned to virtual? What challenges persist?
- We **pulse the workforce** by asking questions such as: Do employees want to come back to an office? Are they more comfortable staying at home due to health risk factors or other reasons? Who cannot work from home due to space, technology access, or confidentiality concerns?
- We **scenario-plan the workplace** by considering questions like: How isolated are individuals' workspaces from others and, if they return to the office, could they operate with minimal contact with other employees? What are likely public health guidelines, including continued social distancing and varying models on location-based outbreaks?

As a firm, we asked ourselves these questions and ultimately used the answers to prepare to make strategic decisions about the landscape of the workplace – and, in turn, how we needed to adjust technology, policies, skills, jobs, performance management, and collaboration tools to enable a blended (co-located and virtual) workforce over the next 12 to 18 months, and beyond. Which brings us to the third phase of our approach, which is Thrive.

**Thrive**: We will iterate and improve upon capabilities that benefit our mission-critical efforts as the Future of Work evolves. This means we will continue to evaluate our work, workforce, and workplace and continue to adapt to meet the needs of our employees and clients. This phase won't end – it is continuous improvement and iteration in response to our evolving global environment and a move towards proactive action, rather than reaction.

## OUR LEARNINGS & RECOMMENDATIONS

Key learnings from our own experience, as well as advising numerous government, commercial, and academic clients through similar conversations, focus on four key areas for this subcommittee's consideration: **IT infrastructure & cybersecurity, real estate & location footprint, performance management, and employee engagement.**

### *IT Infrastructure and Cybersecurity*

Work is more than a set of activities; it is the way people interact, create, learn, grow, team and innovate to produce value-based outcomes. Choosing the correct technologies to enable value-based outcomes requires a holistic picture of where the puck is headed. COVID-19 caused organizations to pivot to a virtual environment rapidly and in doing so they needed to address some fundamental questions:

- Are our employees equipped with necessary technology (e.g. hardware, software, remote tools, data, documents), and do they have the necessary internet and broadband access to support all work-related activities?
- Does our organization have appropriate measures in place, like VPN connections, multi-factor authentication, remote administration of devices, and a robust cybersecurity operations center to ensure people can work remotely on enterprise files and sensitive data safely?

Organizations that were able to answer 'yes' to these questions were better prepared for this rapid virtual transition, further highlighting that investments in IT infrastructure and cybersecurity are critical to organizational agility and adaptability.

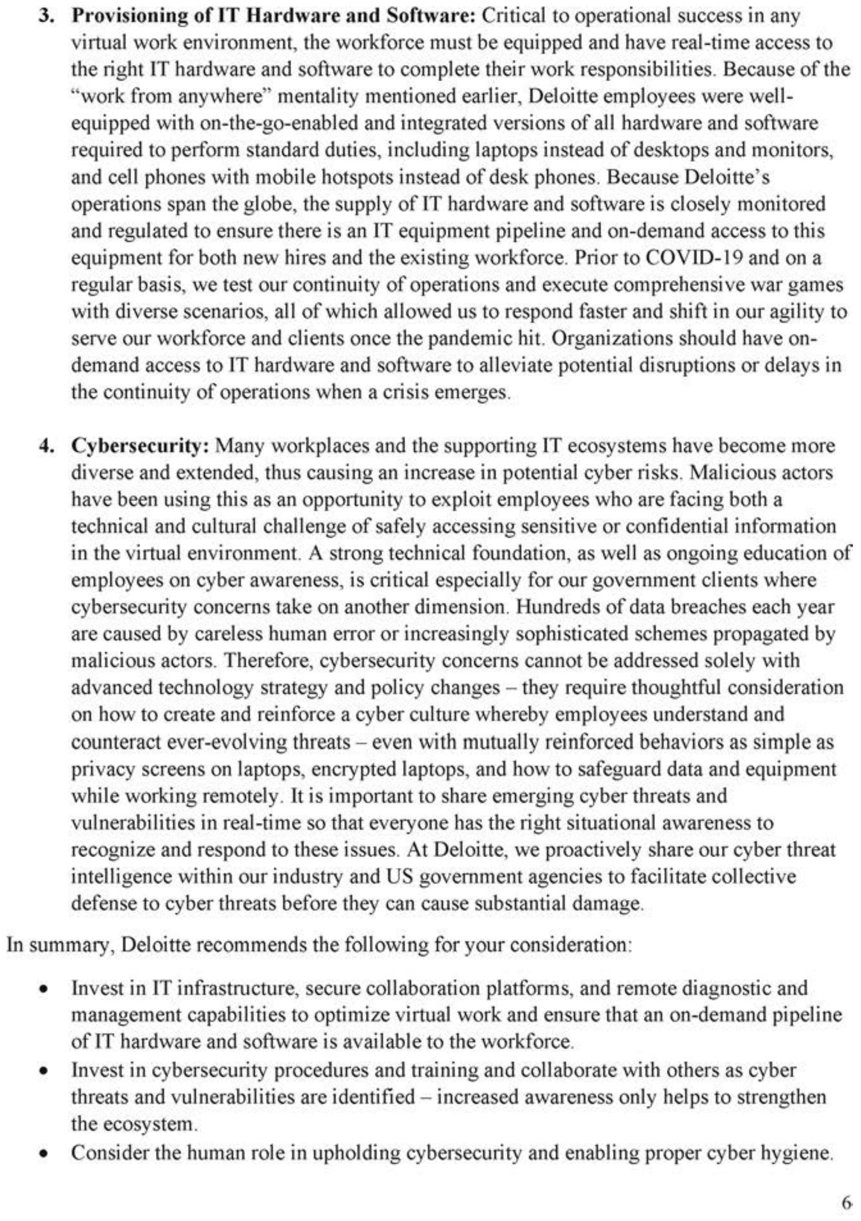
When we went virtual in early March of 2020, we focused on the following key areas, critical to operational success across the globe:

1. **IT Infrastructure and Technology Platforms:** Organizations that were able to successfully make the shift to virtual work had the right IT infrastructure in place to support an entire workforce operating in a virtual environment. Deloitte has made significant investments in both building a robust IT infrastructure and leveraging the breadth of technology capabilities in the current marketplace to operate in a virtual environment. We've done this by utilizing commercial off-the-shelf software and platforms that are configured to a variety of our needs, including communication & collaboration tools, tools for knowledge management and file sharing/storage, workflow management, and data management (including data analytics and visualization tools). Harnessing the full power of these technology capabilities already deployed, Deloitte's workforce was able to seamlessly make the shift to a fully virtual environment and continue to serve clients utilizing multiple technology tools and platforms. A key prerequisite to the successful transition was doing capacity planning and live world testing to confirm that our infrastructure could manage the increased workload.

   With fewer physical and geographic barriers, organizations are acclimating to serving clients from anywhere at any time. At Deloitte we embraced an "employee first" service model years ago and in so doing have stood up IT infrastructure platforms that support both virtual service and self-service. Recognizing the importance of government missions in serving citizens, an equally flexible model of citizen-centered services in a virtual environment should also inform the right IT infrastructure platforms.

   Over the past five years, increasingly cost-effective cloud-based solutions that are designed for quick implementations and scale-up and scale-down scenarios have become more readily available to the government. These solutions formed the backbone of Deloitte's capability to quickly scale our virtual operations during COVID-19. Areas of focus to enable these platforms to work for the government include streamlined procurement processes and standard technical protocols.

2. **Broadband Connectivity and Access:** Deloitte is prepared to work virtually from anywhere by equipping our workforce with cellphones that have real-time access to broadband anywhere in the country. An important component of being able to work virtually is access to reliable broadband to collaborate and serve customers. We recognize that broadband connectivity and access is very important to our clients and the transition to virtual work has really accelerated this need. Any workforce will need access to reliable broadband to successfully perform their work and serve customers in a virtual environment.



3. **Provisioning of IT Hardware and Software:** Critical to operational success in any virtual work environment, the workforce must be equipped and have real-time access to the right IT hardware and software to complete their work responsibilities. Because of the "work from anywhere" mentality mentioned earlier, Deloitte employees were well-equipped with on-the-go-enabled and integrated versions of all hardware and software required to perform standard duties, including laptops instead of desktops and monitors, and cell phones with mobile hotspots instead of desk phones. Because Deloitte's operations span the globe, the supply of IT hardware and software is closely monitored and regulated to ensure there is an IT equipment pipeline and on-demand access to this equipment for both new hires and the existing workforce. Prior to COVID-19 and on a regular basis, we test our continuity of operations and execute comprehensive war games with diverse scenarios, all of which allowed us to respond faster and shift in our agility to serve our workforce and clients once the pandemic hit. Organizations should have on-demand access to IT hardware and software to alleviate potential disruptions or delays in the continuity of operations when a crisis emerges.

4. **Cybersecurity:** Many workplaces and the supporting IT ecosystems have become more diverse and extended, thus causing an increase in potential cyber risks. Malicious actors have been using this as an opportunity to exploit employees who are facing both a technical and cultural challenge of safely accessing sensitive or confidential information in the virtual environment. A strong technical foundation, as well as ongoing education of employees on cyber awareness, is critical especially for our government clients where cybersecurity concerns take on another dimension. Hundreds of data breaches each year are caused by careless human error or increasingly sophisticated schemes propagated by malicious actors. Therefore, cybersecurity concerns cannot be addressed solely with advanced technology strategy and policy changes – they require thoughtful consideration on how to create and reinforce a cyber culture whereby employees understand and counteract ever-evolving threats – even with mutually reinforced behaviors as simple as privacy screens on laptops, encrypted laptops, and how to safeguard data and equipment while working remotely. It is important to share emerging cyber threats and vulnerabilities in real-time so that everyone has the right situational awareness to recognize and respond to these issues. At Deloitte, we proactively share our cyber threat intelligence within our industry and US government agencies to facilitate collective defense to cyber threats before they can cause substantial damage.

In summary, Deloitte recommends the following for your consideration:

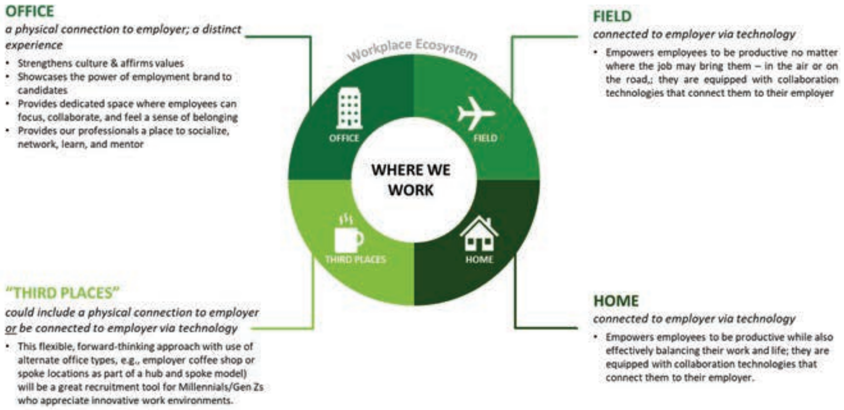
- Invest in IT infrastructure, secure collaboration platforms, and remote diagnostic and management capabilities to optimize virtual work and ensure that an on-demand pipeline of IT hardware and software is available to the workforce.
- Invest in cybersecurity procedures and training and collaborate with others as cyber threats and vulnerabilities are identified – increased awareness only helps to strengthen the ecosystem.
- Consider the human role in upholding cybersecurity and enabling proper cyber hygiene.

### *Real Estate and Location Footprint*

As noted earlier, Deloitte's existing "work from anywhere" environment has shaped our approach to real estate and planning and positioned us to think more innovatively about the broader workplace impacts of more widespread virtual work. For years, our real estate strategy has focused on transitioning us to flexible office spaces that support our workforce's unique and varying needs, with open seating and comfortable collaboration spaces easily reserved via a user-friendly app that shows real-time availability. This concept of 'hoteling' means that practitioners can truly work from anywhere, without being tied to a specific desk. Over time, like many organizations, we had already planned to provide an increasingly flexible offering of locations where employees may choose to work, which likely will decrease our traditional footprint.

Now more than ever, our workplace is a combination of where people work and collaborate to enable the most productive work and the best workforce experience – it has transitioned from a one-size-fits-all office space of cubicles where each employee is expected to spend their week, to a broader set of options in workplaces that form a **workforce ecosystem** responsive to the preferences of employees and the needs of the work.

As organizations look to offer more flexibility in location footprint for their employees, we see four main elements in this ecosystem, as depicted below in *Figure 2* below. First, the traditional office is transformed into a community hub where employees come to collaborate, counsel, and connect. Next, the field is where employees are empowered to be productive no matter where their work may take them. Then there is the home, which is where employees can balance work and life while maintaining productivity – and the primary working location during COVID-19. Finally, a growing set of "Third Places" includes alternative office types that will appeal to the next generation of the workforce that favors innovative and flexible work environments. In sum, we are seeing **location liberation** – the concept that the workplace is not limited to any single physical environment in order to achieve the same outcome or provide the same experience to the employee.



**OFFICE**

*a physical connection to employer; a distinct experience*

- Strengthens culture & affirms values
- Showcases the power of employment brand to candidates
- Provides dedicated space where employees can focus, collaborate, and feel a sense of belonging
- Provides our professionals a place to socialize, network, learn, and mentor

**FIELD**

*connected to employer via technology*

- Empowers employees to be productive no matter where the job may bring them – in the air or on the road,; they are equipped with collaboration technologies that connect them to their employer

**"THIRD PLACES"**

*could include a physical connection to employer or be connected to employer via technology*

- This flexible, forward-thinking approach with use of alternate office types, e.g., employer coffee shop or spoke locations as part of a hub and spoke model) will be a great recruitment tool for Millennials/Gen Zs who appreciate innovative work environments.

**HOME**

*connected to employer via technology*

- Empowers employees to be productive while also effectively balancing their work and life; they are equipped with collaboration technologies that connect them to their employer.

*Figure 2: The Workforce Ecosystem*

In summary, Deloitte recommends the following for your consideration:

- Reimagine the workplace ecosystem at the organizational level to provide multiple, flexible options for where and how government employees conduct their work.
- Build a work-from-anywhere culture that empowers employees to maintain productivity while also achieving work-life balance.

### *Performance Management*

An effective performance management approach is a core foundational element for building trust between supervisors and employees, and for focusing progress toward organizational and mission success. Deloitte's approach to performance management is grounded in frequent, meaningful conversations to fuel the performance and development of our people and teams. These conversations, when coupled with reliable data and insights, enable us to understand and recognize performance throughout the year.

The rapid transition to virtual work presents government organizations with an opportunity to challenge the orthodoxy that physical presence and visibility in the office equals a productive and high-performing workforce. Utilizing an effective performance framework that gathers and measures feedback across all levels in the organization, supervisors can measure outcomes, create a culture of feedback, and elevate the workforce experience. Virtual and distributed working require us to expand our lens of productivity by focusing on work effectiveness, work efficiency, and workforce empowerment. Employers must be proactive and explicit in making the desired outcomes and outputs of work visible to employees in order to achieve them. Shifting to measuring accomplishments and outcomes over activities and labor hours allows organizations to cultivate a work environment of high-performing and productive teams.

Performance management approaches focused on an annual event (such as a year-end performance review) miss the opportunity for a more well-rounded view of performance resulting from a series of regular check-ins with multiple team leaders, co-workers, and direct reports. Further, performance management approaches that establish a series of performance indicators around qualitative and quantitative outcomes, rather than responsibilities, allow for a more effective measurement of how an employee is performing.

In summary, Deloitte recommends the following for your consideration:

- Use this as an opportunity to implement a new performance management approach which assesses meaningful qualitative and quantitative metrics focused on outcomes and provides opportunities for frequent check-ins to discuss both the work itself and the overall work experience.
- Cultivate a culture of continuous 360 feedback, clear expectations, and open communication to increase trust between supervisors and employees.

***Employee Engagement***

In my experience, an employee's engagement level is highest the first day they start a job and can progressively decline if the work experience fails to meet expectations. According to our 2020 Global Human Capital trends survey, 86% of employees and executives cite lack of collaboration or ineffective communication for workplace failures. Therefore, organizations like Deloitte invest heavily in an employee's experience from the recruiting phase all the way through to our alumni program. This full life cycle investment is widely recognized as enabling higher returns on attracting and retaining the most diverse and highly skilled workforce in addition to the highest levels of mission effectiveness and productivity.

Challenging moments like COVID-19 can result in significant declines to employee engagement when leaders and organizations fail to adapt their strategies. At Deloitte we are utilizing the challenges presented by working remotely during COVID-19 as an opportunity to take a deeper dive into what our people are experiencing as we strive to create the number one talent experience. For example, we are working with cohorts such as underrepresented minorities and caregivers to identify areas of challenge in their work experiences and proactively rectifying them. We are creating forums and utilizing point-in-time "pulse surveys" to gather input and discuss current events and concerns so our people have an outlet for their voice to be heard. Since the onset of COVID-19, we have transitioned and expanded many of our learning, social impact, and team-building events to virtual platforms to ensure that this important input of employee engagement continues to build momentum. The impact that remote work has on even the most fundamental learning moments on the job – from onboarding, to system training, to working with teams – cannot be understated, and the rapid virtualization of learning programs is a complex challenge for any organization. The future of learning must provide workers with easy access to digitally enabled learning resources, on demand. At Deloitte, we took on the issue of opening access to learning using enabling environments that empower the workforce to access and curate learning that is available inside and outside the organization. And, in a time when "working from home" can often be interpreted as "working all the time," we are closely monitoring paid time off and actively encouraging our people to take time off and manage the balance between their working time and the time they are taking for their own well-being. We've been successful at preserving our productivity and client delivery because we have put our employees at the center of our Respond, Recover, and Thrive framework.

We are using the necessity of working from home in response to COVID-19 as an opportunity to double down on employee engagement to strengthen our future. By assessing, prioritizing, and developing timely strategies to match work activities to the workplace, we are rethinking the work for years to come. This, in turn, allows us to refresh and expand the concept of "employee experience" to address the "human experience" at work. We recognize that elevating the human experience in a virtual work environment includes hands-on management, establishing a positive work environment, providing meaningful work, allowing growth opportunities, and instilling trust in leadership.

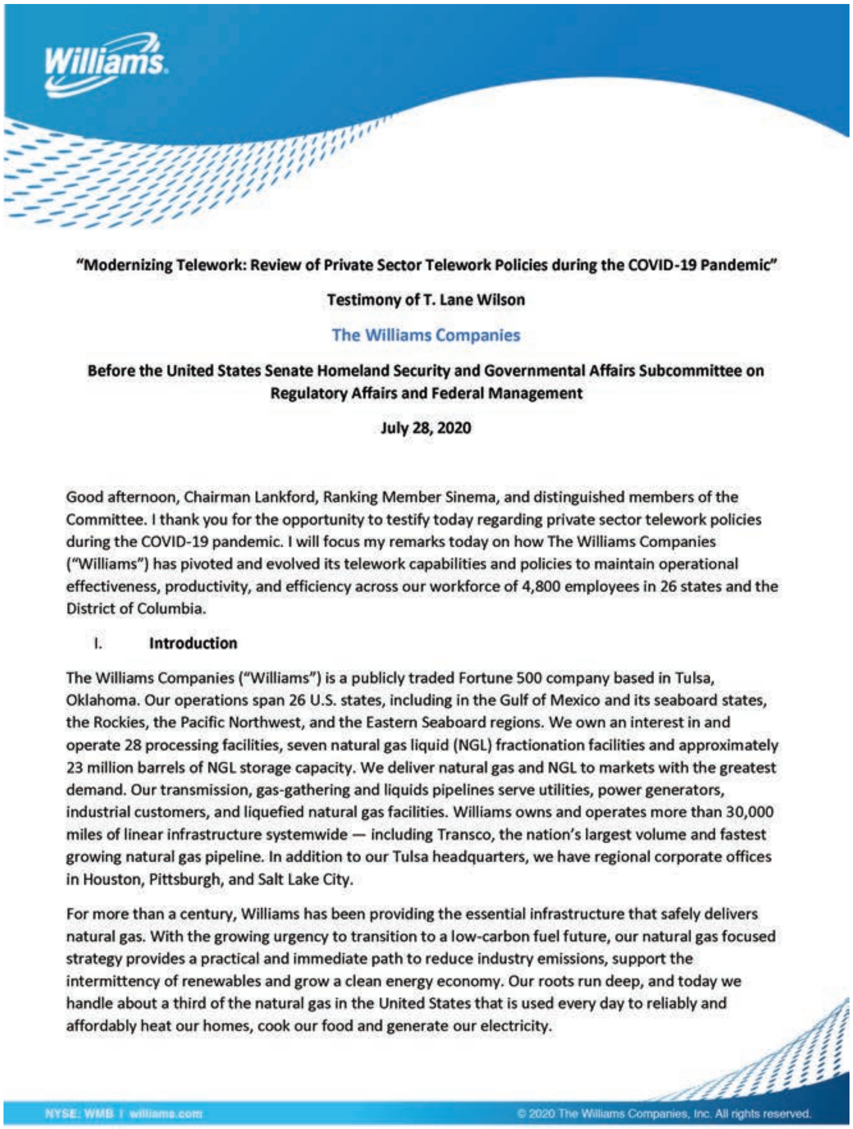
In summary, Deloitte recommends the following for your consideration:

- Prioritize open, honest conversations about culture and employee morale at all levels.
- Invest in digital capabilities that provide a shared and standardized employee experience for the entire workforce, across all work locations.
- Build structures that provide hands-on management and positive work environments for both virtual and in-person employee experiences.

**CONCLUSION**

The fundamental principle underlying all four of these key areas is one we embody at Deloitte and support our clients in as well: an organization must fundamentally consider its human capital to be its core asset. Considering the critical roles of IT & cybersecurity, real estate, performance management, and employee engagement during the continued evolution of virtual work post-COVID-19 and beyond have enabled Deloitte – and, we believe, can enable the government – to turn this challenge into an opportunity, and accelerate towards the future.

Thank you again for providing me this opportunity to share Deloitte's perspectives on this topic. I look forward to answering your questions.



**“Modernizing Telework: Review of Private Sector Telework Policies during the COVID-19 Pandemic”**

**Testimony of T. Lane Wilson**

**The Williams Companies**

**Before the United States Senate Homeland Security and Governmental Affairs Subcommittee on Regulatory Affairs and Federal Management**

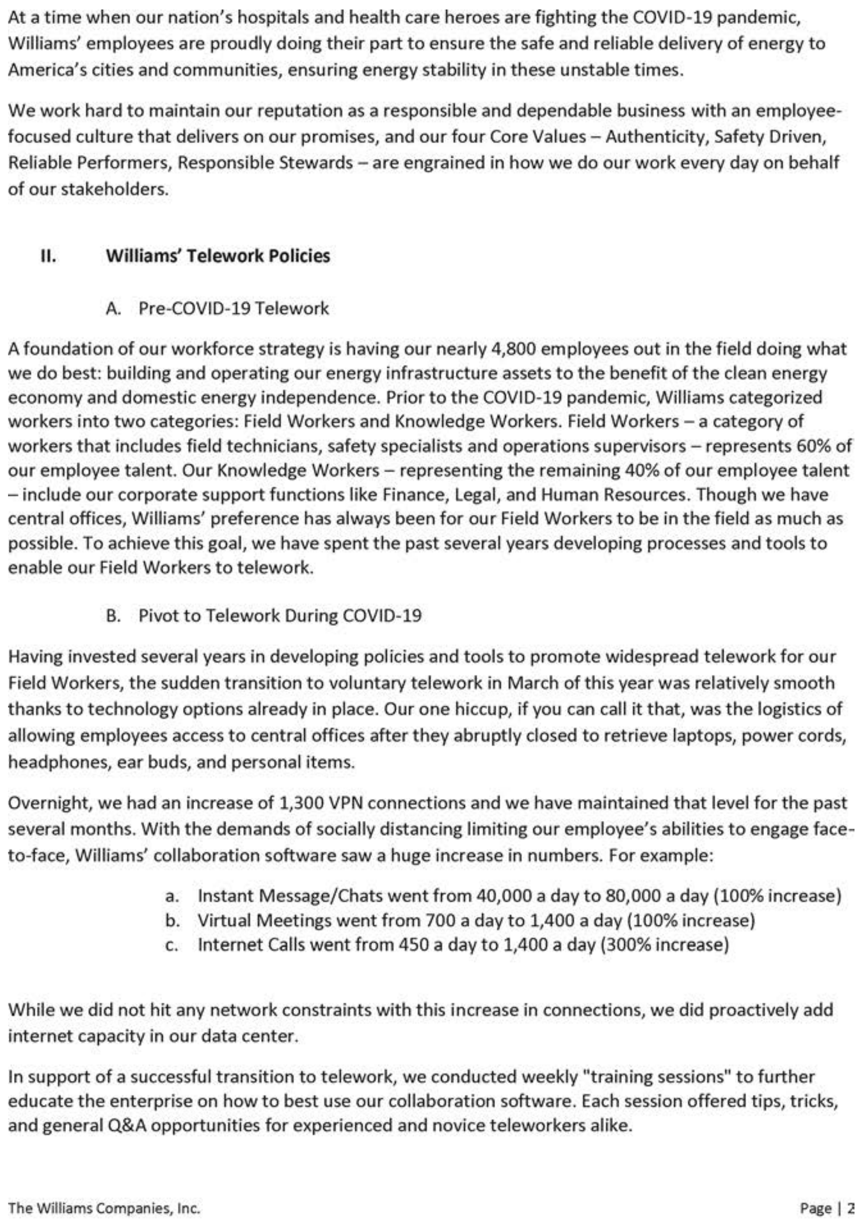
**July 28, 2020**

Good afternoon, Chairman Lankford, Ranking Member Sinema, and distinguished members of the Committee. I thank you for the opportunity to testify today regarding private sector telework policies during the COVID-19 pandemic. I will focus my remarks today on how The Williams Companies (“Williams”) has pivoted and evolved its telework capabilities and policies to maintain operational effectiveness, productivity, and efficiency across our workforce of 4,800 employees in 26 states and the District of Columbia.

## I. Introduction

The Williams Companies (“Williams”) is a publicly traded Fortune 500 company based in Tulsa, Oklahoma. Our operations span 26 U.S. states, including in the Gulf of Mexico and its seaboard states, the Rockies, the Pacific Northwest, and the Eastern Seaboard regions. We own an interest in and operate 28 processing facilities, seven natural gas liquid (NGL) fractionation facilities and approximately 23 million barrels of NGL storage capacity. We deliver natural gas and NGL to markets with the greatest demand. Our transmission, gas-gathering and liquids pipelines serve utilities, power generators, industrial customers, and liquefied natural gas facilities. Williams owns and operates more than 30,000 miles of linear infrastructure systemwide — including Transco, the nation’s largest volume and fastest growing natural gas pipeline. In addition to our Tulsa headquarters, we have regional corporate offices in Houston, Pittsburgh, and Salt Lake City.

For more than a century, Williams has been providing the essential infrastructure that safely delivers natural gas. With the growing urgency to transition to a low-carbon fuel future, our natural gas focused strategy provides a practical and immediate path to reduce industry emissions, support the intermittency of renewables and grow a clean energy economy. Our roots run deep, and today we handle about a third of the natural gas in the United States that is used every day to reliably and affordably heat our homes, cook our food and generate our electricity.



At a time when our nation's hospitals and health care heroes are fighting the COVID-19 pandemic, Williams' employees are proudly doing their part to ensure the safe and reliable delivery of energy to America's cities and communities, ensuring energy stability in these unstable times.

We work hard to maintain our reputation as a responsible and dependable business with an employee-focused culture that delivers on our promises, and our four Core Values – Authenticity, Safety Driven, Reliable Performers, Responsible Stewards – are engrained in how we do our work every day on behalf of our stakeholders.

## II. Williams' Telework Policies

### A. Pre-COVID-19 Telework

A foundation of our workforce strategy is having our nearly 4,800 employees out in the field doing what we do best: building and operating our energy infrastructure assets to the benefit of the clean energy economy and domestic energy independence. Prior to the COVID-19 pandemic, Williams categorized workers into two categories: Field Workers and Knowledge Workers. Field Workers – a category of workers that includes field technicians, safety specialists and operations supervisors – represents 60% of our employee talent. Our Knowledge Workers – representing the remaining 40% of our employee talent – include our corporate support functions like Finance, Legal, and Human Resources. Though we have central offices, Williams' preference has always been for our Field Workers to be in the field as much as possible. To achieve this goal, we have spent the past several years developing processes and tools to enable our Field Workers to telework.

### B. Pivot to Telework During COVID-19

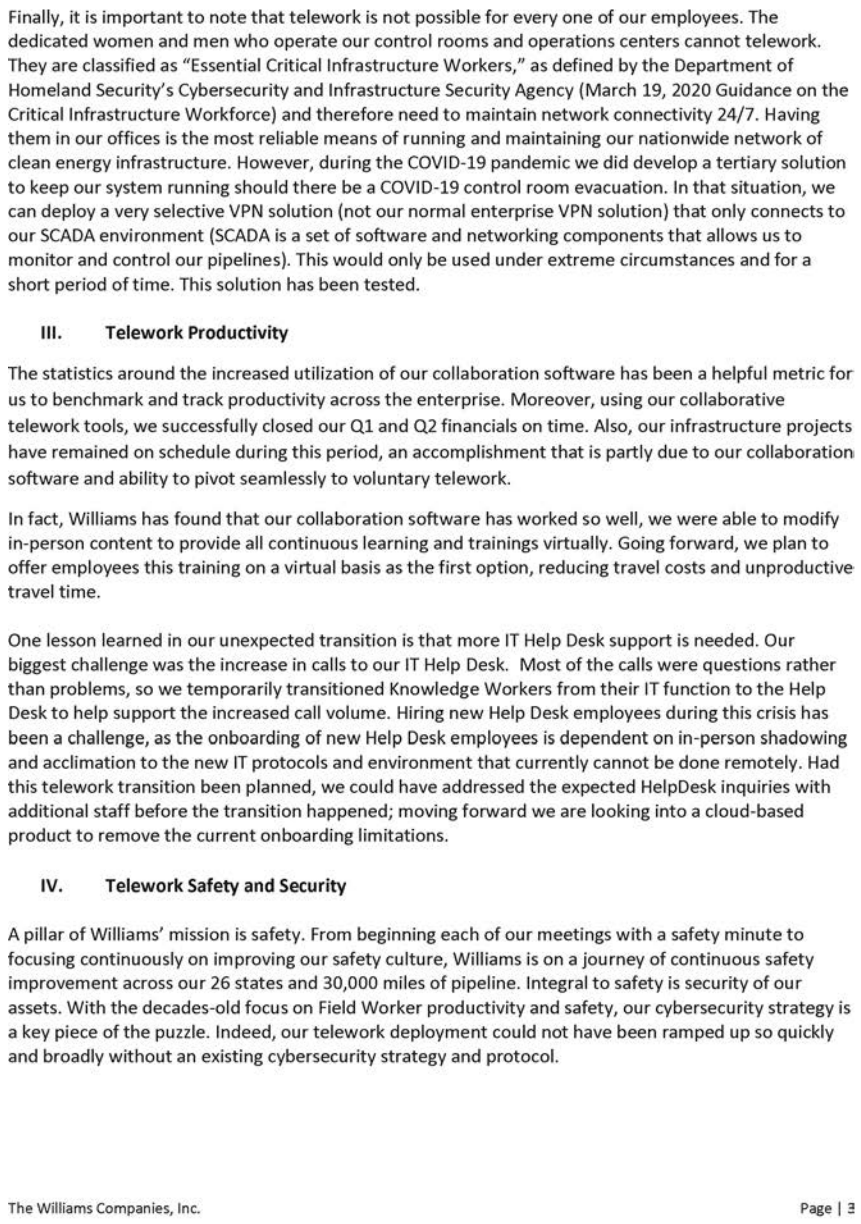
Having invested several years in developing policies and tools to promote widespread telework for our Field Workers, the sudden transition to voluntary telework in March of this year was relatively smooth thanks to technology options already in place. Our one hiccup, if you can call it that, was the logistics of allowing employees access to central offices after they abruptly closed to retrieve laptops, power cords, headphones, ear buds, and personal items.

Overnight, we had an increase of 1,300 VPN connections and we have maintained that level for the past several months. With the demands of socially distancing limiting our employee's abilities to engage face-to-face, Williams' collaboration software saw a huge increase in numbers. For example:

a. Instant Message/Chats went from 40,000 a day to 80,000 a day (100% increase)
b. Virtual Meetings went from 700 a day to 1,400 a day (100% increase)
c. Internet Calls went from 450 a day to 1,400 a day (300% increase)

While we did not hit any network constraints with this increase in connections, we did proactively add internet capacity in our data center.

In support of a successful transition to telework, we conducted weekly "training sessions" to further educate the enterprise on how to best use our collaboration software. Each session offered tips, tricks, and general Q&A opportunities for experienced and novice teleworkers alike.



Finally, it is important to note that telework is not possible for every one of our employees. The dedicated women and men who operate our control rooms and operations centers cannot telework. They are classified as "Essential Critical Infrastructure Workers," as defined by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (March 19, 2020 Guidance on the Critical Infrastructure Workforce) and therefore need to maintain network connectivity 24/7. Having them in our offices is the most reliable means of running and maintaining our nationwide network of clean energy infrastructure. However, during the COVID-19 pandemic we did develop a tertiary solution to keep our system running should there be a COVID-19 control room evacuation. In that situation, we can deploy a very selective VPN solution (not our normal enterprise VPN solution) that only connects to our SCADA environment (SCADA is a set of software and networking components that allows us to monitor and control our pipelines). This would only be used under extreme circumstances and for a short period of time. This solution has been tested.

## III. Telework Productivity

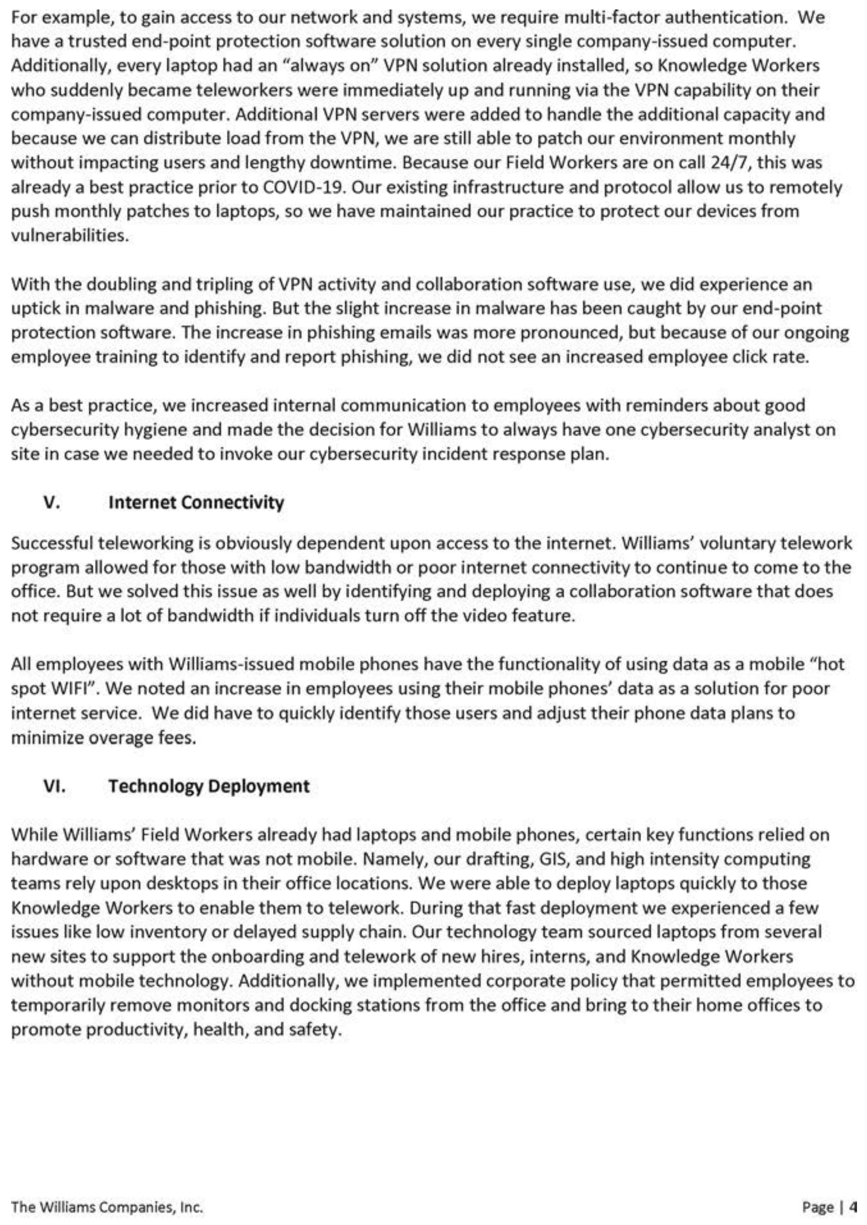
The statistics around the increased utilization of our collaboration software has been a helpful metric for us to benchmark and track productivity across the enterprise. Moreover, using our collaborative telework tools, we successfully closed our Q1 and Q2 financials on time. Also, our infrastructure projects have remained on schedule during this period, an accomplishment that is partly due to our collaboration software and ability to pivot seamlessly to voluntary telework.

In fact, Williams has found that our collaboration software has worked so well, we were able to modify in-person content to provide all continuous learning and trainings virtually. Going forward, we plan to offer employees this training on a virtual basis as the first option, reducing travel costs and unproductive travel time.

One lesson learned in our unexpected transition is that more IT Help Desk support is needed. Our biggest challenge was the increase in calls to our IT Help Desk. Most of the calls were questions rather than problems, so we temporarily transitioned Knowledge Workers from their IT function to the Help Desk to help support the increased call volume. Hiring new Help Desk employees during this crisis has been a challenge, as the onboarding of new Help Desk employees is dependent on in-person shadowing and acclimation to the new IT protocols and environment that currently cannot be done remotely. Had this telework transition been planned, we could have addressed the expected HelpDesk inquiries with additional staff before the transition happened; moving forward we are looking into a cloud-based product to remove the current onboarding limitations.

## IV. Telework Safety and Security

A pillar of Williams' mission is safety. From beginning each of our meetings with a safety minute to focusing continuously on improving our safety culture, Williams is on a journey of continuous safety improvement across our 26 states and 30,000 miles of pipeline. Integral to safety is security of our assets. With the decades-old focus on Field Worker productivity and safety, our cybersecurity strategy is a key piece of the puzzle. Indeed, our telework deployment could not have been ramped up so quickly and broadly without an existing cybersecurity strategy and protocol.



For example, to gain access to our network and systems, we require multi-factor authentication. We have a trusted end-point protection software solution on every single company-issued computer. Additionally, every laptop had an “always on” VPN solution already installed, so Knowledge Workers who suddenly became teleworkers were immediately up and running via the VPN capability on their company-issued computer. Additional VPN servers were added to handle the additional capacity and because we can distribute load from the VPN, we are still able to patch our environment monthly without impacting users and lengthy downtime. Because our Field Workers are on call 24/7, this was already a best practice prior to COVID-19. Our existing infrastructure and protocol allow us to remotely push monthly patches to laptops, so we have maintained our practice to protect our devices from vulnerabilities.

With the doubling and tripling of VPN activity and collaboration software use, we did experience an uptick in malware and phishing. But the slight increase in malware has been caught by our end-point protection software. The increase in phishing emails was more pronounced, but because of our ongoing employee training to identify and report phishing, we did not see an increased employee click rate.

As a best practice, we increased internal communication to employees with reminders about good cybersecurity hygiene and made the decision for Williams to always have one cybersecurity analyst on site in case we needed to invoke our cybersecurity incident response plan.

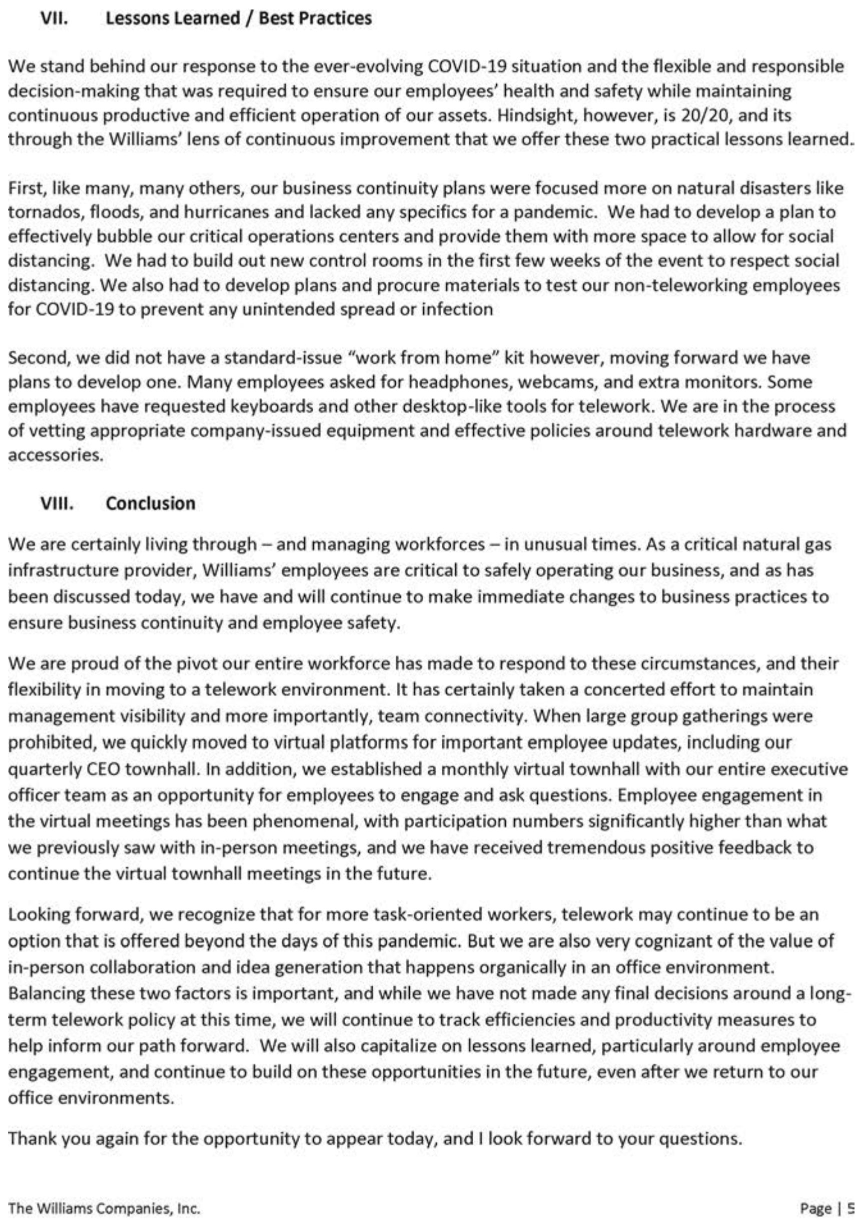
## V. Internet Connectivity

Successful teleworking is obviously dependent upon access to the internet. Williams’ voluntary telework program allowed for those with low bandwidth or poor internet connectivity to continue to come to the office. But we solved this issue as well by identifying and deploying a collaboration software that does not require a lot of bandwidth if individuals turn off the video feature.

All employees with Williams-issued mobile phones have the functionality of using data as a mobile “hot spot WIFI”. We noted an increase in employees using their mobile phones’ data as a solution for poor internet service. We did have to quickly identify those users and adjust their phone data plans to minimize overage fees.

## VI. Technology Deployment

While Williams’ Field Workers already had laptops and mobile phones, certain key functions relied on hardware or software that was not mobile. Namely, our drafting, GIS, and high intensity computing teams rely upon desktops in their office locations. We were able to deploy laptops quickly to those Knowledge Workers to enable them to telework. During that fast deployment we experienced a few issues like low inventory or delayed supply chain. Our technology team sourced laptops from several new sites to support the onboarding and telework of new hires, interns, and Knowledge Workers without mobile technology. Additionally, we implemented corporate policy that permitted employees to temporarily remove monitors and docking stations from the office and bring to their home offices to promote productivity, health, and safety.



### VII. Lessons Learned / Best Practices

We stand behind our response to the ever-evolving COVID-19 situation and the flexible and responsible decision-making that was required to ensure our employees' health and safety while maintaining continuous productive and efficient operation of our assets. Hindsight, however, is 20/20, and its through the Williams' lens of continuous improvement that we offer these two practical lessons learned.

First, like many, many others, our business continuity plans were focused more on natural disasters like tornados, floods, and hurricanes and lacked any specifics for a pandemic. We had to develop a plan to effectively bubble our critical operations centers and provide them with more space to allow for social distancing. We had to build out new control rooms in the first few weeks of the event to respect social distancing. We also had to develop plans and procure materials to test our non-teleworking employees for COVID-19 to prevent any unintended spread or infection

Second, we did not have a standard-issue "work from home" kit however, moving forward we have plans to develop one. Many employees asked for headphones, webcams, and extra monitors. Some employees have requested keyboards and other desktop-like tools for telework. We are in the process of vetting appropriate company-issued equipment and effective policies around telework hardware and accessories.

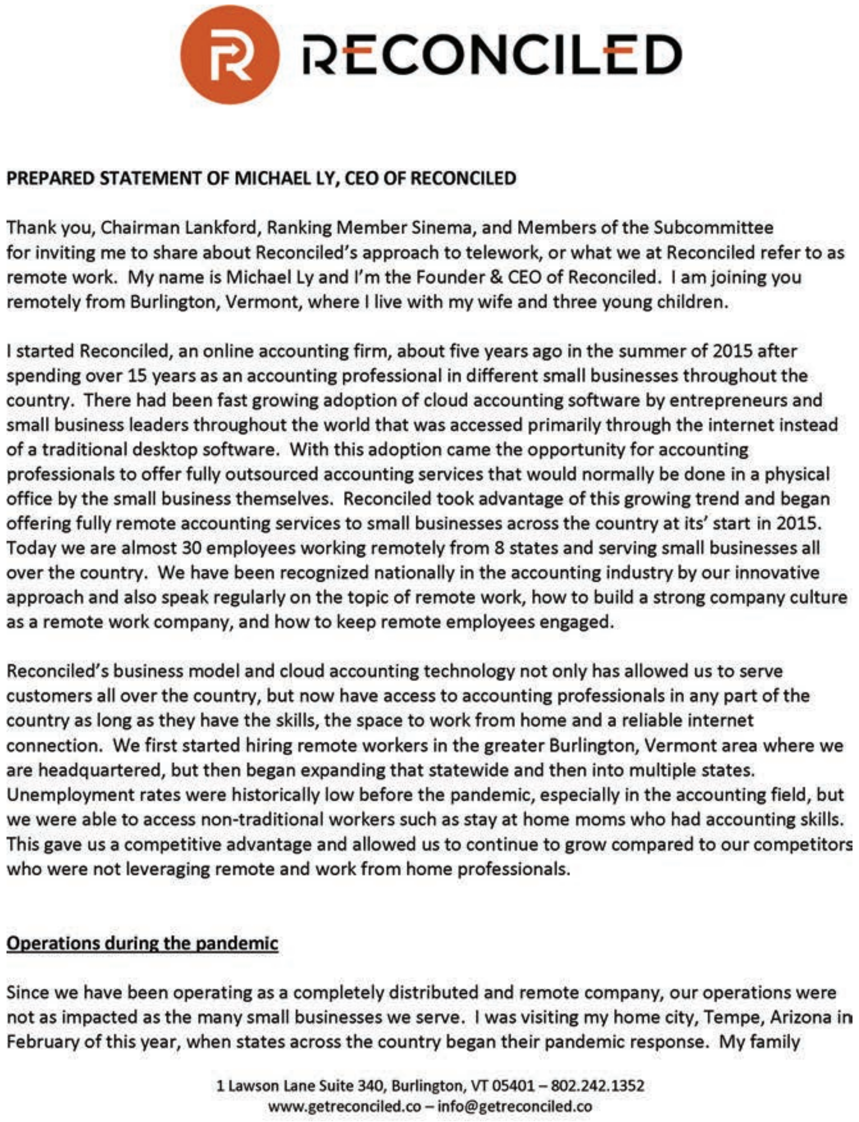
### VIII. Conclusion

We are certainly living through – and managing workforces – in unusual times. As a critical natural gas infrastructure provider, Williams' employees are critical to safely operating our business, and as has been discussed today, we have and will continue to make immediate changes to business practices to ensure business continuity and employee safety.

We are proud of the pivot our entire workforce has made to respond to these circumstances, and their flexibility in moving to a telework environment. It has certainly taken a concerted effort to maintain management visibility and more importantly, team connectivity. When large group gatherings were prohibited, we quickly moved to virtual platforms for important employee updates, including our quarterly CEO townhall. In addition, we established a monthly virtual townhall with our entire executive officer team as an opportunity for employees to engage and ask questions. Employee engagement in the virtual meetings has been phenomenal, with participation numbers significantly higher than what we previously saw with in-person meetings, and we have received tremendous positive feedback to continue the virtual townhall meetings in the future.

Looking forward, we recognize that for more task-oriented workers, telework may continue to be an option that is offered beyond the days of this pandemic. But we are also very cognizant of the value of in-person collaboration and idea generation that happens organically in an office environment. Balancing these two factors is important, and while we have not made any final decisions around a long-term telework policy at this time, we will continue to track efficiencies and productivity measures to help inform our path forward. We will also capitalize on lessons learned, particularly around employee engagement, and continue to build on these opportunities in the future, even after we return to our office environments.

Thank you again for the opportunity to appear today, and I look forward to your questions.



RECONCILED

**PREPARED STATEMENT OF MICHAEL LY, CEO OF RECONCILED**

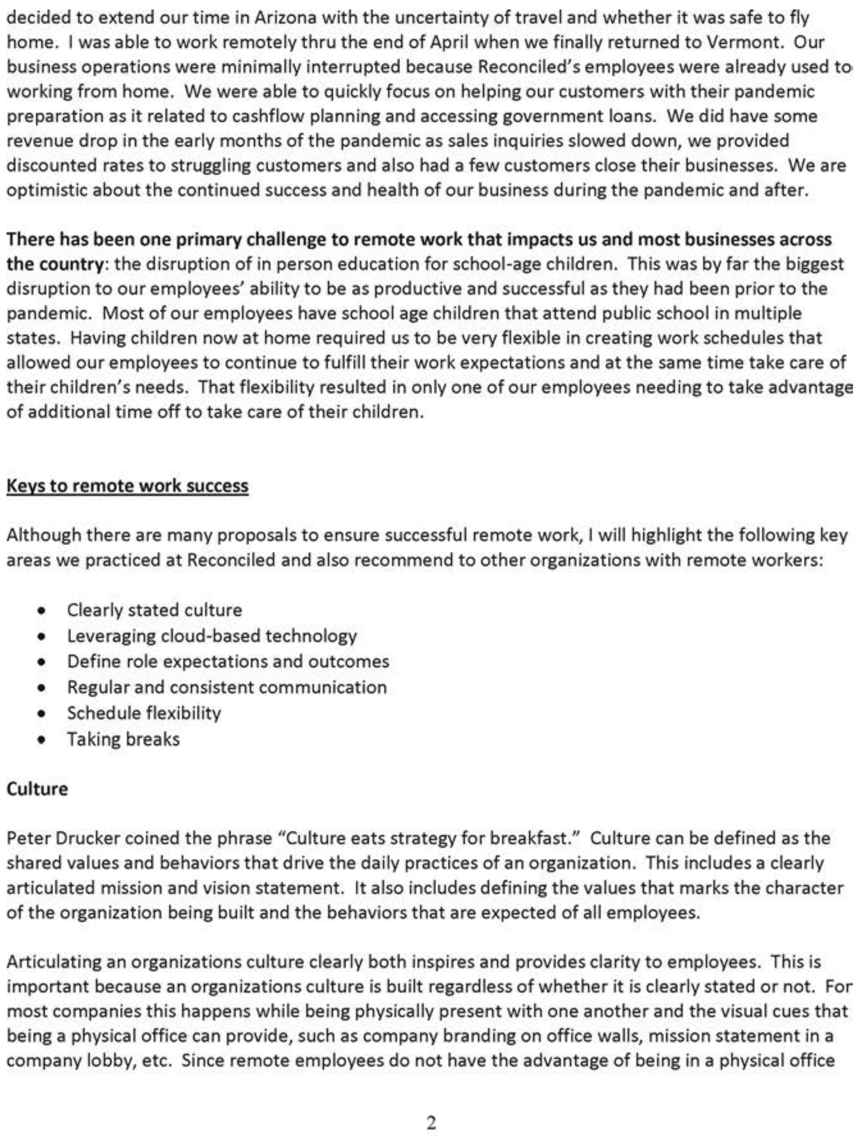
Thank you, Chairman Lankford, Ranking Member Sinema, and Members of the Subcommittee for inviting me to share about Reconciled's approach to telework, or what we at Reconciled refer to as remote work. My name is Michael Ly and I'm the Founder & CEO of Reconciled. I am joining you remotely from Burlington, Vermont, where I live with my wife and three young children.

I started Reconciled, an online accounting firm, about five years ago in the summer of 2015 after spending over 15 years as an accounting professional in different small businesses throughout the country. There had been fast growing adoption of cloud accounting software by entrepreneurs and small business leaders throughout the world that was accessed primarily through the internet instead of a traditional desktop software. With this adoption came the opportunity for accounting professionals to offer fully outsourced accounting services that would normally be done in a physical office by the small business themselves. Reconciled took advantage of this growing trend and began offering fully remote accounting services to small businesses across the country at its' start in 2015. Today we are almost 30 employees working remotely from 8 states and serving small businesses all over the country. We have been recognized nationally in the accounting industry by our innovative approach and also speak regularly on the topic of remote work, how to build a strong company culture as a remote work company, and how to keep remote employees engaged.

Reconciled's business model and cloud accounting technology not only has allowed us to serve customers all over the country, but now have access to accounting professionals in any part of the country as long as they have the skills, the space to work from home and a reliable internet connection. We first started hiring remote workers in the greater Burlington, Vermont area where we are headquartered, but then began expanding that statewide and then into multiple states. Unemployment rates were historically low before the pandemic, especially in the accounting field, but we were able to access non-traditional workers such as stay at home moms who had accounting skills. This gave us a competitive advantage and allowed us to continue to grow compared to our competitors who were not leveraging remote and work from home professionals.

**Operations during the pandemic**

Since we have been operating as a completely distributed and remote company, our operations were not as impacted as the many small businesses we serve. I was visiting my home city, Tempe, Arizona in February of this year, when states across the country began their pandemic response. My family



decided to extend our time in Arizona with the uncertainty of travel and whether it was safe to fly home. I was able to work remotely thru the end of April when we finally returned to Vermont. Our business operations were minimally interrupted because Reconciled's employees were already used to working from home. We were able to quickly focus on helping our customers with their pandemic preparation as it related to cashflow planning and accessing government loans. We did have some revenue drop in the early months of the pandemic as sales inquiries slowed down, we provided discounted rates to struggling customers and also had a few customers close their businesses. We are optimistic about the continued success and health of our business during the pandemic and after.

**There has been one primary challenge to remote work that impacts us and most businesses across the country**: the disruption of in person education for school-age children. This was by far the biggest disruption to our employees' ability to be as productive and successful as they had been prior to the pandemic. Most of our employees have school age children that attend public school in multiple states. Having children now at home required us to be very flexible in creating work schedules that allowed our employees to continue to fulfill their work expectations and at the same time take care of their children's needs. That flexibility resulted in only one of our employees needing to take advantage of additional time off to take care of their children.

## Keys to remote work success

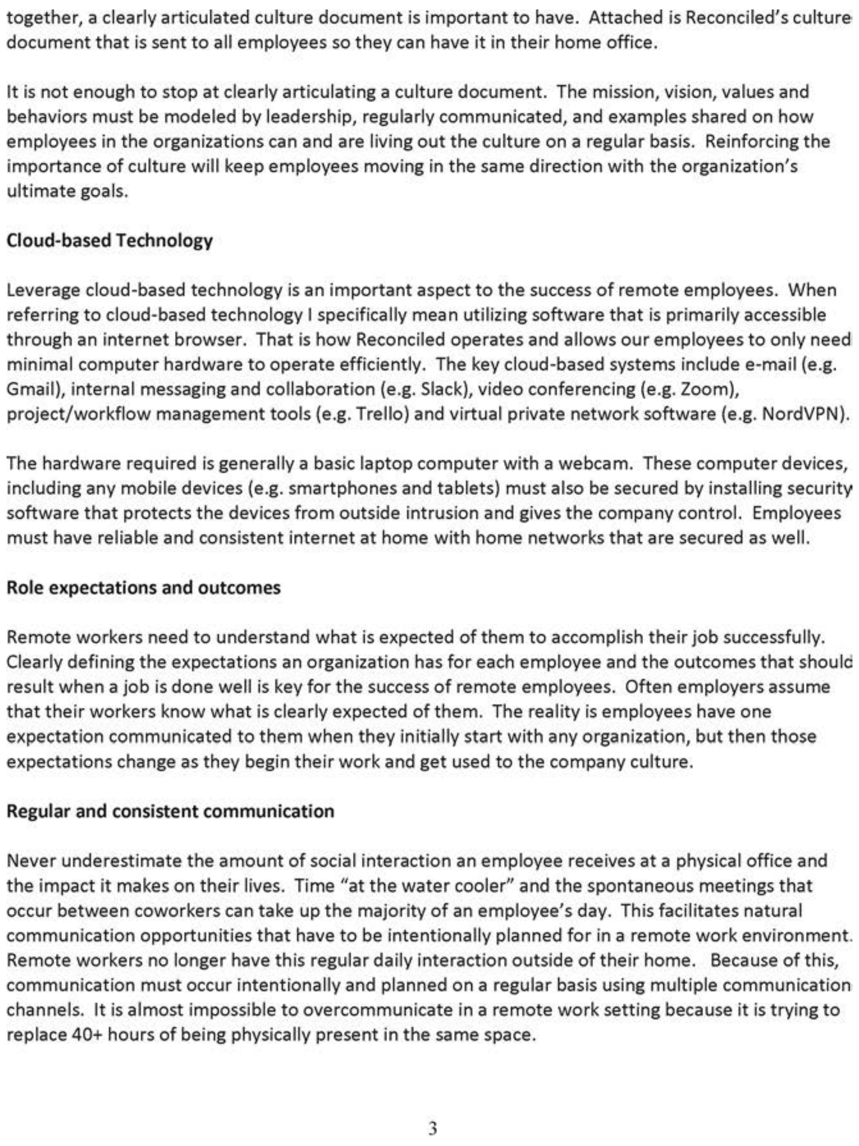
Although there are many proposals to ensure successful remote work, I will highlight the following key areas we practiced at Reconciled and also recommend to other organizations with remote workers:

- Clearly stated culture
- Leveraging cloud-based technology
- Define role expectations and outcomes
- Regular and consistent communication
- Schedule flexibility
- Taking breaks

### Culture

Peter Drucker coined the phrase "Culture eats strategy for breakfast." Culture can be defined as the shared values and behaviors that drive the daily practices of an organization. This includes a clearly articulated mission and vision statement. It also includes defining the values that marks the character of the organization being built and the behaviors that are expected of all employees.

Articulating an organizations culture clearly both inspires and provides clarity to employees. This is important because an organizations culture is built regardless of whether it is clearly stated or not. For most companies this happens while being physically present with one another and the visual cues that being a physical office can provide, such as company branding on office walls, mission statement in a company lobby, etc. Since remote employees do not have the advantage of being in a physical office



together, a clearly articulated culture document is important to have. Attached is Reconciled's culture document that is sent to all employees so they can have it in their home office.

It is not enough to stop at clearly articulating a culture document. The mission, vision, values and behaviors must be modeled by leadership, regularly communicated, and examples shared on how employees in the organizations can and are living out the culture on a regular basis. Reinforcing the importance of culture will keep employees moving in the same direction with the organization's ultimate goals.

**Cloud-based Technology**

Leverage cloud-based technology is an important aspect to the success of remote employees. When referring to cloud-based technology I specifically mean utilizing software that is primarily accessible through an internet browser. That is how Reconciled operates and allows our employees to only need minimal computer hardware to operate efficiently. The key cloud-based systems include e-mail (e.g. Gmail), internal messaging and collaboration (e.g. Slack), video conferencing (e.g. Zoom), project/workflow management tools (e.g. Trello) and virtual private network software (e.g. NordVPN).

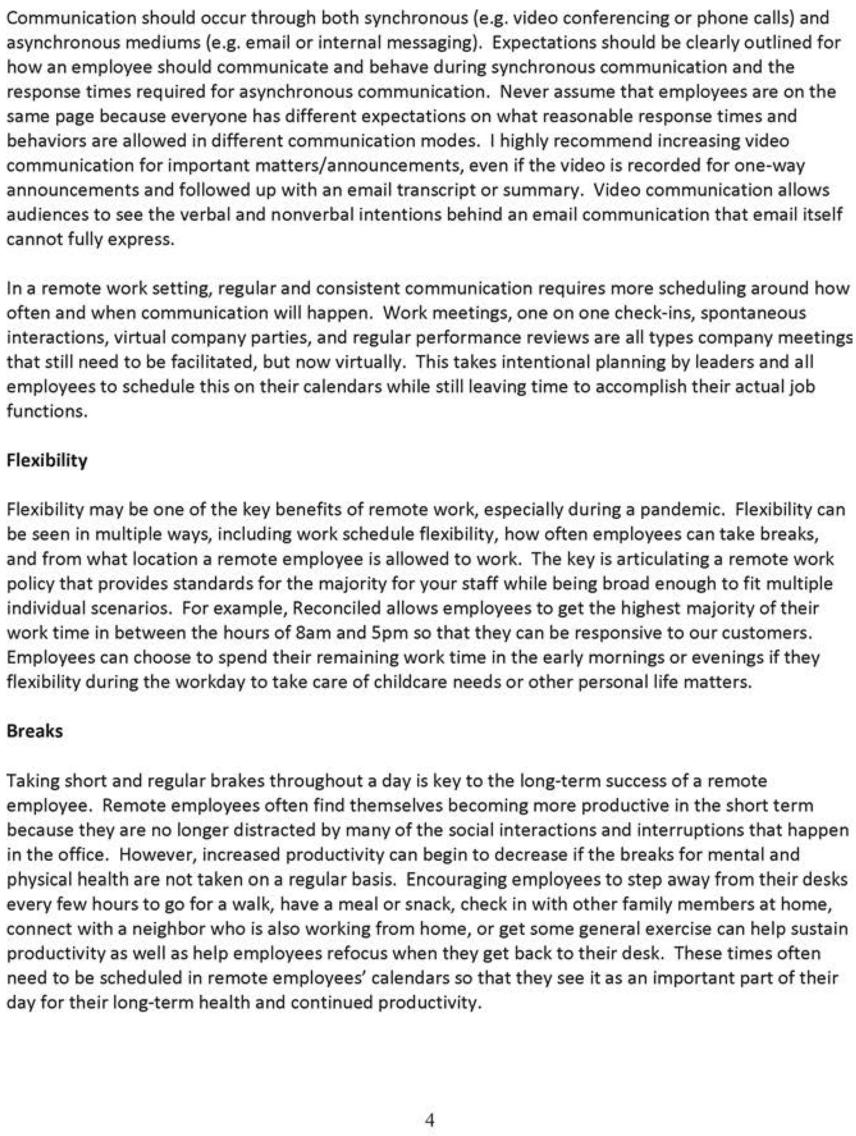
The hardware required is generally a basic laptop computer with a webcam. These computer devices, including any mobile devices (e.g. smartphones and tablets) must also be secured by installing security software that protects the devices from outside intrusion and gives the company control. Employees must have reliable and consistent internet at home with home networks that are secured as well.

**Role expectations and outcomes**

Remote workers need to understand what is expected of them to accomplish their job successfully. Clearly defining the expectations an organization has for each employee and the outcomes that should result when a job is done well is key for the success of remote employees. Often employers assume that their workers know what is clearly expected of them. The reality is employees have one expectation communicated to them when they initially start with any organization, but then those expectations change as they begin their work and get used to the company culture.

**Regular and consistent communication**

Never underestimate the amount of social interaction an employee receives at a physical office and the impact it makes on their lives. Time "at the water cooler" and the spontaneous meetings that occur between coworkers can take up the majority of an employee's day. This facilitates natural communication opportunities that have to be intentionally planned for in a remote work environment. Remote workers no longer have this regular daily interaction outside of their home. Because of this, communication must occur intentionally and planned on a regular basis using multiple communication channels. It is almost impossible to overcommunicate in a remote work setting because it is trying to replace 40+ hours of being physically present in the same space.



Communication should occur through both synchronous (e.g. video conferencing or phone calls) and asynchronous mediums (e.g. email or internal messaging). Expectations should be clearly outlined for how an employee should communicate and behave during synchronous communication and the response times required for asynchronous communication. Never assume that employees are on the same page because everyone has different expectations on what reasonable response times and behaviors are allowed in different communication modes. I highly recommend increasing video communication for important matters/announcements, even if the video is recorded for one-way announcements and followed up with an email transcript or summary. Video communication allows audiences to see the verbal and nonverbal intentions behind an email communication that email itself cannot fully express.

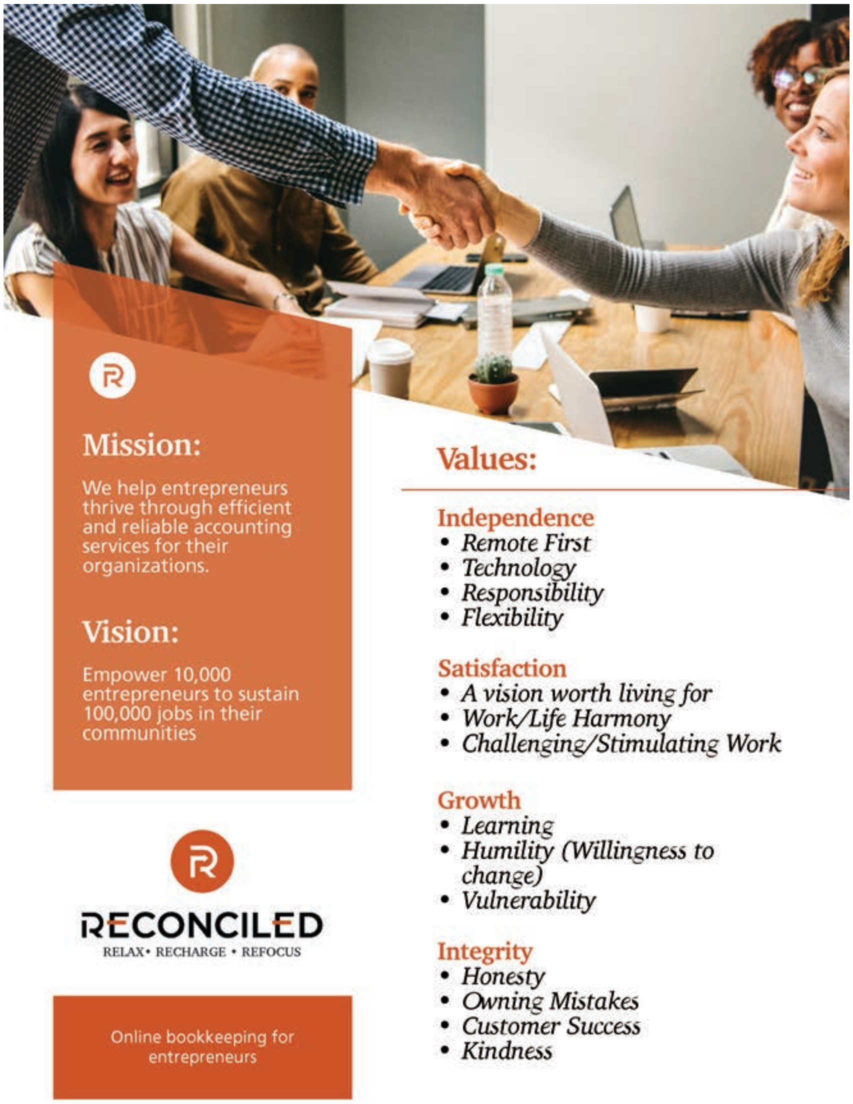
In a remote work setting, regular and consistent communication requires more scheduling around how often and when communication will happen. Work meetings, one on one check-ins, spontaneous interactions, virtual company parties, and regular performance reviews are all types company meetings that still need to be facilitated, but now virtually. This takes intentional planning by leaders and all employees to schedule this on their calendars while still leaving time to accomplish their actual job functions.

**Flexibility**

Flexibility may be one of the key benefits of remote work, especially during a pandemic. Flexibility can be seen in multiple ways, including work schedule flexibility, how often employees can take breaks, and from what location a remote employee is allowed to work. The key is articulating a remote work policy that provides standards for the majority for your staff while being broad enough to fit multiple individual scenarios. For example, Reconciled allows employees to get the highest majority of their work time in between the hours of 8am and 5pm so that they can be responsive to our customers. Employees can choose to spend their remaining work time in the early mornings or evenings if they flexibility during the workday to take care of childcare needs or other personal life matters.

**Breaks**

Taking short and regular brakes throughout a day is key to the long-term success of a remote employee. Remote employees often find themselves becoming more productive in the short term because they are no longer distracted by many of the social interactions and interruptions that happen in the office. However, increased productivity can begin to decrease if the breaks for mental and physical health are not taken on a regular basis. Encouraging employees to step away from their desks every few hours to go for a walk, have a meal or snack, check in with other family members at home, connect with a neighbor who is also working from home, or get some general exercise can help sustain productivity as well as help employees refocus when they get back to their desk. These times often need to be scheduled in remote employees' calendars so that they see it as an important part of their day for their long-term health and continued productivity.



## Mission:

We help entrepreneurs thrive through efficient and reliable accounting services for their organizations.

## Vision:

Empower 10,000 entrepreneurs to sustain 100,000 jobs in their communities

RECONCILED
RELAX• RECHARGE • REFOCUS

Online bookkeeping for entrepreneurs

## Values:

### Independence

- *Remote First*
- *Technology*
- *Responsibility*
- *Flexibility*

### Satisfaction

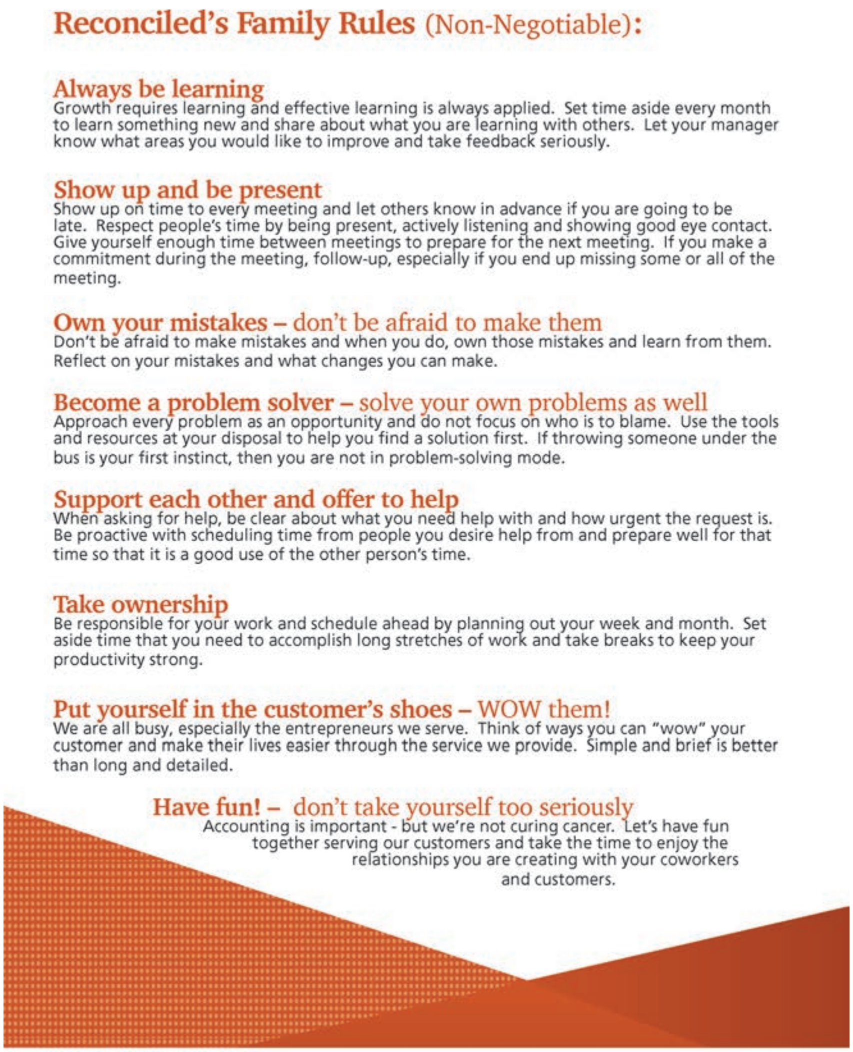
- *A vision worth living for*
- *Work/Life Harmony*
- *Challenging/Stimulating Work*

### Growth

- *Learning*
- *Humility (Willingness to change)*
- *Vulnerability*

### Integrity

- *Honesty*
- *Owning Mistakes*
- *Customer Success*
- *Kindness*



## Reconciled's Family Rules (Non-Negotiable):

### Always be learning

Growth requires learning and effective learning is always applied. Set time aside every month to learn something new and share about what you are learning with others. Let your manager know what areas you would like to improve and take feedback seriously.

### Show up and be present

Show up on time to every meeting and let others know in advance if you are going to be late. Respect people's time by being present, actively listening and showing good eye contact. Give yourself enough time between meetings to prepare for the next meeting. If you make a commitment during the meeting, follow-up, especially if you end up missing some or all of the meeting.

### Own your mistakes – don't be afraid to make them

Don't be afraid to make mistakes and when you do, own those mistakes and learn from them. Reflect on your mistakes and what changes you can make.

### Become a problem solver – solve your own problems as well

Approach every problem as an opportunity and do not focus on who is to blame. Use the tools and resources at your disposal to help you find a solution first. If throwing someone under the bus is your first instinct, then you are not in problem-solving mode.

### Support each other and offer to help

When asking for help, be clear about what you need help with and how urgent the request is. Be proactive with scheduling time from people you desire help from and prepare well for that time so that it is a good use of the other person's time.

### Take ownership

Be responsible for your work and schedule ahead by planning out your week and month. Set aside time that you need to accomplish long stretches of work and take breaks to keep your productivity strong.

### Put yourself in the customer's shoes – WOW them!

We are all busy, especially the entrepreneurs we serve. Think of ways you can "wow" your customer and make their lives easier through the service we provide. Simple and brief is better than long and detailed.

### Have fun! – don't take yourself too seriously

Accounting is important - but we're not curing cancer. Let's have fun together serving our customers and take the time to enjoy the relationships you are creating with your coworkers and customers.

WRITTEN STATEMENT FOR THE RECORD

OF

JOHN ZANNI
CHIEF EXECUTIVE OFFICER
ACRONIS SCS

BEFORE THE

US SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

SUBCOMMITTEE ON REGULATORY AFFAIRS AND FEDERAL MANAGEMENT

ON

"MODERNIZING TELEWORK: REVIEW OF PRIVATE SECTOR TELEWORK POLICIES DURING THE COVID-19 PANDEMIC"

Tuesday, July 28, 2020

## Introduction

Chairman Lankford, Ranking Member Sinema, members of the Committee, it is an honor to join you today. Ranking Member Sinema, thank you for the invitation to come discuss the particular challenges associated with telework, in light of the ongoing COVID-19 pandemic.

Both of you have been instrumental in the Committee's efforts to educate the American people on the Nation's cybersecurity vulnerabilities and have developed bipartisan legislative initiatives that help address them—bills like your *Telework for U.S. Innovation Act* and the *Emergency Telework Act* before it.

With this in mind, I appreciate the opportunity to share my insight—informed by more than two and half decades in the cybersecurity field, including in my current role as Chief Executive Officer of Acronis SCS, an Arizona-based company dedicated to meeting the unique cyber protection and edge data security needs of the US public sector, including federal, state and local government, education, public healthcare, and nonprofit institutions.

## Pre-COVID-19 Context

There is no question: the modern cyber threat landscape is more sophisticated and relentless than ever before. While COVID-19 has brought certain cybersecurity challenges into stark focus, like those associated with 2020's dramatic rise in telework, many of the threats we see reflected in headlines today are not new.

In 2019, for example, nearly one thousand US public sector organizations, including government agencies, education institutions, and healthcare providers, were hit with ransomware attacks, costing upwards of $7.5 billion – and those are just the publicly reported numbers.[1] In total, North America experienced 18,648 cyber incidents in 2019, including almost a thousand data breaches that compromised confidential information.[2]

Put simply, we had an epidemic of a different sort on our hands long before COVID-19, which has now become much more apparent and urgent.

## Understanding Telework Vulnerabilities

The current pandemic has driven a massive move to telework, along with an increased reliance on technology and data outside of controlled environments. With that shift has come a staggering jump in criminal cyber activity from bad actors eager to take advantage of COVID-19 for their own personal, monetary, or geopolitical gain. The fear and confusion of the pandemic presented an opening, in the form of hunger for new information, that has made scams and phishing attempts more successful. To put data to the problem, the number of domains with "corona" or

[1] https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

[2] https://enterprise.verizon.com/resources/reports/dbir/

"covid" in their names jumped from 190 in 2019 to more than 38,000 in March of this year.[3] Some of those websites are legitimate. The vast majority are not.

Since March, we have also seen a jump in scam emails purporting to offer safety tips from seemingly trustworthy sources, like the World Health Organization and US Centers for Disease Control. Once opened, malicious attachments and links introduce ransomware or other attack vectors that can spread throughout an entire network, presenting particular challenges for businesses and public sector organizations trying to keep critical services up-and-running.

The rapid shift to telework in response to the spread of the virus only amplified these and other cyber vulnerabilities. Virtually overnight, employees had to not only stay productive in an entirely new work cadence, but also protect sensitive organizational systems and data while far from the office. IT teams, in turn, scrambled to enable safe and secure telework capabilities, like adding virtual private network (VPN) lines and virtual desktops or deploying collaboration applications, like Microsoft Teams.

In both the private and public sectors, the dislocation between businesses operations and the workforces needed to sustain them that this pandemic has caused has both exacerbated existing cybersecurity vulnerabilities and created new ones. As your recent legislative initiatives recognize, the ability of businesses to survive the already daunting challenges presented by the pandemic will depend, in part, on their ability to adapt to a more mobile workforce with cybersecurity vulnerabilities in mind.

Today's typical home includes a spate of devices: desktops, laptops, tablets, smartphones and gaming consoles, some consumer Internet of Things (IoT) devices like smart TVs and home security systems, and maybe even a few network-connected toys and appliances. All these devices share access to a standard Wi-Fi router with basic security settings. The IT resources and processes we all take for granted in an office – regular patching of operating systems, software, network devices, and security appliances; network safeguards like firewalls and intrusion prevention systems; daily backups of all workloads; updates of endpoint anti-malware and firmware, and; help desk support – are often greatly reduced.

This environment is an obvious risk when employees use personal equipment to access an organization's private network, even with secure VPN connections, particularly when family members without proper security training share access to such devices. However, the home environment can also threaten the security of organization-owned devices, like a company laptop. Any device in the household (including unattended IoT devices) could inadvertently let in a piece of malware that threatens all connected devices, including those accessing the company or organizational network. Worse still, many IoT devices can never be patched for security vulnerabilities, leading to so-called 'forever-day' risks that make them particularly easy and appealing targets for cybercriminals.

The surge in use of videoconferencing and telecommunications applications – like Zoom, WebEx, and Microsoft Teams – has also presented new risks. The typical videoconferencing call

[3] https://intsights.com/resources/covid-19-cyber-threat-impact-report

involves multiple people connecting from home environments, some from personal devices over unsecured networks, into a single session. Without proper protections in place, such applications are vulnerable to message injection and code injection attacks, remote-control hijacking, watering-hole attacks via compromised third-party libraries and applications, session ID hijacking, exploits of outdated versions, man-in-the-middle attacks on chat and video streams, and redirection to malicious URLs.

As IT teams parse through these challenges, the risk of conducting business in such an environment is real. Last year, for example, even before we saw a steep incline in teleworking, thirty-nine percent of companies and fifty-six percent of public sector agencies reported suffering a major mobile or IoT-related compromise.[4]

In spite of such a complex threat landscape though, there is positive news as well: adopting a "defense in depth" approach to telework (and cyber hygiene in general), based on the concept of layered protection, will greatly diminish such risks. Simple tools and relatively easy-to-deploy processes, described in more detail below, are available to help organizations implement such an approach in their own environments.

**A Successful Shift to Telework**

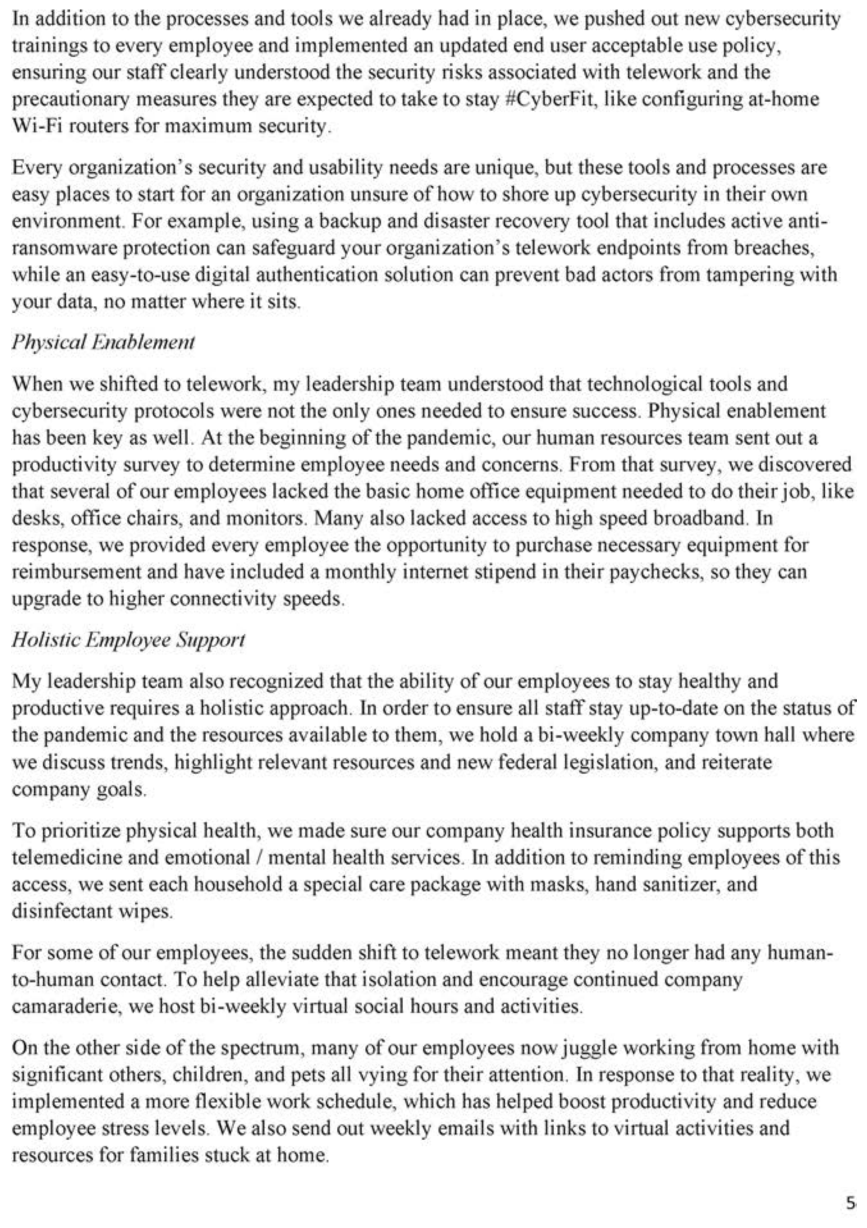
As the CEO of a cyber protection and edge data security company, I had two primary priorities when the pandemic hit. The first was ensuring the safety of my employees, both physically and digitally, as we transitioned to a full telework posture starting in mid-March. The second was adjusting our processes to support customers in need of future-proof solutions that would help their own organizations stay safe not only during the pandemic, but long after.

*Technical Enablement & Cybersecurity*

I am fortunate that Acronis SCS was already well positioned for telework before the pandemic hit. All our employees had company laptops equipped with anti-virus/anti-malware protections, as well as a regular backup schedule. Acronis SCS also adheres to a strict zero trust framework, applied across the enterprise – from our office and data centers to our network, applications, endpoints, email, and cloud infrastructure. We leverage next-generation firewalls and segment our networks based on the least privilege access model. We also use a tool to prevent email-based malware incursions, as well as require multi-factor authentication (MFA) and certificate-based VPN for access to certain sensitive resources.

This layered "defense in depth" posture helped us easily shift to telework without disruptions or fear that an attack on one device would compromise the whole company. For example, each remote employee only has access to one company network rather than all. If their system is infiltrated, the impact will be narrowly contained.

[4] https://enterprise.verizon.com/resources/reports/mobile-security-index/



In addition to the processes and tools we already had in place, we pushed out new cybersecurity trainings to every employee and implemented an updated end user acceptable use policy, ensuring our staff clearly understood the security risks associated with telework and the precautionary measures they are expected to take to stay #CyberFit, like configuring at-home Wi-Fi routers for maximum security.

Every organization's security and usability needs are unique, but these tools and processes are easy places to start for an organization unsure of how to shore up cybersecurity in their own environment. For example, using a backup and disaster recovery tool that includes active anti-ransomware protection can safeguard your organization's telework endpoints from breaches, while an easy-to-use digital authentication solution can prevent bad actors from tampering with your data, no matter where it sits.

*Physical Enablement*

When we shifted to telework, my leadership team understood that technological tools and cybersecurity protocols were not the only ones needed to ensure success. Physical enablement has been key as well. At the beginning of the pandemic, our human resources team sent out a productivity survey to determine employee needs and concerns. From that survey, we discovered that several of our employees lacked the basic home office equipment needed to do their job, like desks, office chairs, and monitors. Many also lacked access to high speed broadband. In response, we provided every employee the opportunity to purchase necessary equipment for reimbursement and have included a monthly internet stipend in their paychecks, so they can upgrade to higher connectivity speeds.

*Holistic Employee Support*

My leadership team also recognized that the ability of our employees to stay healthy and productive requires a holistic approach. In order to ensure all staff stay up-to-date on the status of the pandemic and the resources available to them, we hold a bi-weekly company town hall where we discuss trends, highlight relevant resources and new federal legislation, and reiterate company goals.

To prioritize physical health, we made sure our company health insurance policy supports both telemedicine and emotional / mental health services. In addition to reminding employees of this access, we sent each household a special care package with masks, hand sanitizer, and disinfectant wipes.

For some of our employees, the sudden shift to telework meant they no longer had any human-to-human contact. To help alleviate that isolation and encourage continued company camaraderie, we host bi-weekly virtual social hours and activities.

On the other side of the spectrum, many of our employees now juggle working from home with significant others, children, and pets all vying for their attention. In response to that reality, we implemented a more flexible work schedule, which has helped boost productivity and reduce employee stress levels. We also send out weekly emails with links to virtual activities and resources for families stuck at home.

### *Productivity Factors*

In addition to adopting more flexible hours, the company prioritized other productivity-enhancing measures as well. We updated our management objectives system to better outline and measure employee performance. With an eye towards resilience, we ensured every member of the team had a backup person well-versed in their job duties, in case someone got sick and had to take time off to recover.

We also made virtual engagement and impromptu meetings just as easily accessible to employees as they would be in office. For example, our sales and customer support teams keep a Zoom group chat open all day long, to facilitate collaboration and cross-team communication.

### *Continued Customer Focus*

In addition to adopting new policies and practices to better support our employees, when the pandemic hit, we also doubled down on our commitment to provide software that meets the unique security and usability needs of US public sector entities, whether that be an agency keeping mission critical assets, like industrial control and weapons systems, up-and-running, or a municipality protecting new telework endpoints, like employee laptops and phones.

We have stayed up-to-date on the challenges our customers face as they adjust to remote work realities, such as adding hundreds of thousands of new VPN lines, deploying thousands of remote desktops, or even considering expanded bring-your-own-device (BYOD) policies for affordability reasons. We have also taken every opportunity available to help amplify understanding of vulnerabilities (like the risk of turning off VPN or MFA, for example) and educate our customers and the wider public on cybersecurity best practices.

We also released a new solution in April, Acronis SCS Cyber Protect Cloud, designed to help organizations address telework challenges. The offering combines reliable backup and disaster recovery, full-stack anti-malware protection, and endpoint security and management capabilities (like automatic patching, remote desktop, and Zoom security) in one easy-to-navigate management console.

## Increased Urgency

The rise in telework has brought with it a spate of challenges – but it has also renewed urgency to better address those challenges with more future-proof approaches. I want to thank the Homeland Security and Governmental Affairs Committee for its efforts to bring cyber hygiene issues to the forefront of the legislature's priority list and Americans' minds.

In 2020 alone, this Committee has introduced six bills directly relating to cybersecurity and two more regarding federal telework policies. That level of urgency is absolutely critical. Ranking Member Sinema, as the leader of a Scottsdale-based company, I must also express my sincere thanks for your leadership to ensure Arizona is secure, including your co-sponsorship of the *Cybersecurity State Coordinator Act* earlier this year.

From the recommendations outlined in this year's Cyberspace Solarium Commission Report, several of which I am encouraged to see have been incorporated into NDAA amendments or introduced as bills, to the Department of Defense's much-needed Cybersecurity Maturation Model Certification (CMMC), all signs point to increased urgency and impactful change – and a more secure Nation and robust economy as a result.

This growing urgency on cybersecurity in general lays the groundwork for more future-proof responses to telework vulnerabilities in particular. This is not a private sector or public sector concern. As our society and institutions become more interconnected, a breach or attack on one will have reverberating impacts on all. Moving forward, as issues like unemployment and healthcare dominate discussions of the COVID-19 response, America cannot afford to relegate cybersecurity to the back-burner. The risks of doing so are simply too high.

### A Practical Framework for Building Digital Resiliency

As the urgency to address critical vulnerabilities and policy gaps grows, our Nation's public and private sectors need a cyber hygiene framework that promotes long-term digital resilience over quick fixes.

With healthcare top of mind, we can use that industry's model to prevent and treat illnesses as inspiration for the type of dynamic cyber protection plan organizations of all shapes and sizes must adopt – a plan which considers the inevitability of attack and identifies what policies and practices are needed to quickly and effectively recover.

**Prevention** – Like vaccines that proactively prevent illness, cyber protection tools and processes like vulnerability assessment, patch management, regular backup schedules, continuous data protection, and a zero trust architecture are key for helping companies and government agencies maintain cyber hygiene across all endpoints and prevent critical downtime and data loss.

**Detection** – Similar to the testing that takes place in the medical field, IT teams must employ artificial intelligence (AI) based threat detection and behavioral analysis (like URL filtering) on all endpoints and systems, so abnormalities can be easily and quickly identified.

**Response** – Once an illness is discovered, doctors can administer medication in response. Similar steps must be taken when an attack, hardware failure, or human error occurs on the cyber front. IT teams should streamline the response process by employing automated alert and remediation tools that allow for real-time reactions and triage.

**Recovery** – When illnesses or injuries become serious, doctors may perform surgery to help a patient recover. Similarly, once a cyber incident occurs, IT teams must focus on quickly restoring systems and avoiding the devastating downtime and data loss that could spell disaster.

**Forensics** – After an illness or injury is discovered, the medical community conducts extensive research to better understand the ailment and what can be done to treat it more effectively moving forward. Such post-incident investigation and analysis are equally as critical in the cyber realm. After an attack or failure occurs (an inevitability for every institution, no matter how good its prevention methods are), IT teams and end users alike must understand the causes of the incident – and how to avoid something similar in the future.

**Conclusion**

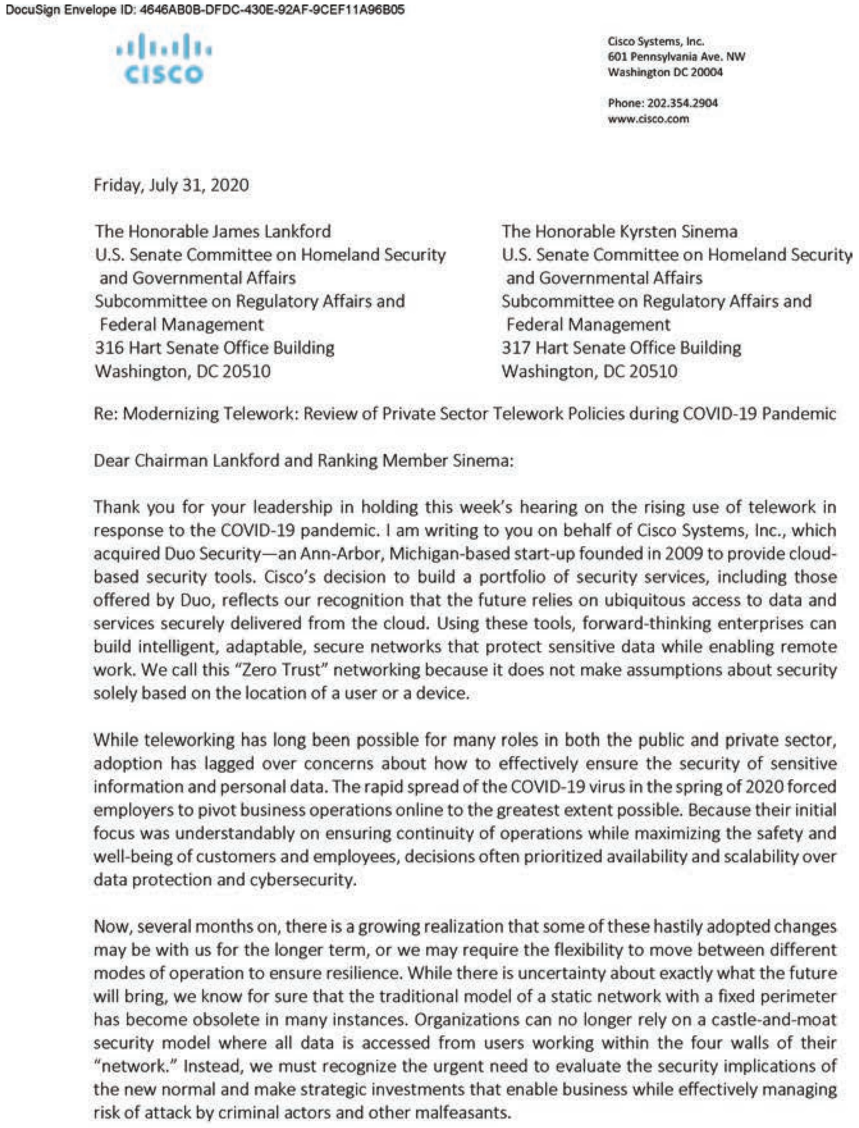
Whether COVID-19 subsides next week or next year, it is clear that increased telework flexibility is in America's long-term future. In light of the threat landscape described above, there is little time to waste in building digital resiliency and strengthening cyber hygiene.

Far too often, commercial and government needs are placed at odds with one another when it comes to cybersecurity. That reality must change – but it will take more buy in and collaboration from all sides of the equation, including private companies, Congress, and federal, state, and local government agencies. On the private sector side, companies must make a more robust commitment to consider public sector needs when developing solutions to cyber challenges. My experience at the helm of Acronis SCS has taught me that doing so is not always the easiest or most profitable route, but it is the right one for ensuring our national security and prosperity.

To close, I would like to borrow a few of Ranking Member Sinema's words from April of last year: "The United States must do a better job of developing cybersecurity standards, educating users about the cyber risks and solutions for connected devices, and increasing transparency for consumers." I could not agree more – and both I and Acronis SCS stand ready to serve as committed partners in that effort.

Chairman Lankford, Ranking Member Sinema, members of the Committee, thank you again for the opportunity to be here today. I look forward to hearing your insights and addressing your questions.

###



DocuSign Envelope ID: 4646AB0B-DFDC-430E-92AF-9CEF11A96B05

Cisco Systems, Inc.
601 Pennsylvania Ave. NW
Washington DC 20004

Phone: 202.354.2904
www.cisco.com

Friday, July 31, 2020

The Honorable James Lankford
U.S. Senate Committee on Homeland Security
and Governmental Affairs
Subcommittee on Regulatory Affairs and
Federal Management
316 Hart Senate Office Building
Washington, DC 20510

The Honorable Kyrsten Sinema
U.S. Senate Committee on Homeland Security
and Governmental Affairs
Subcommittee on Regulatory Affairs and
Federal Management
317 Hart Senate Office Building
Washington, DC 20510

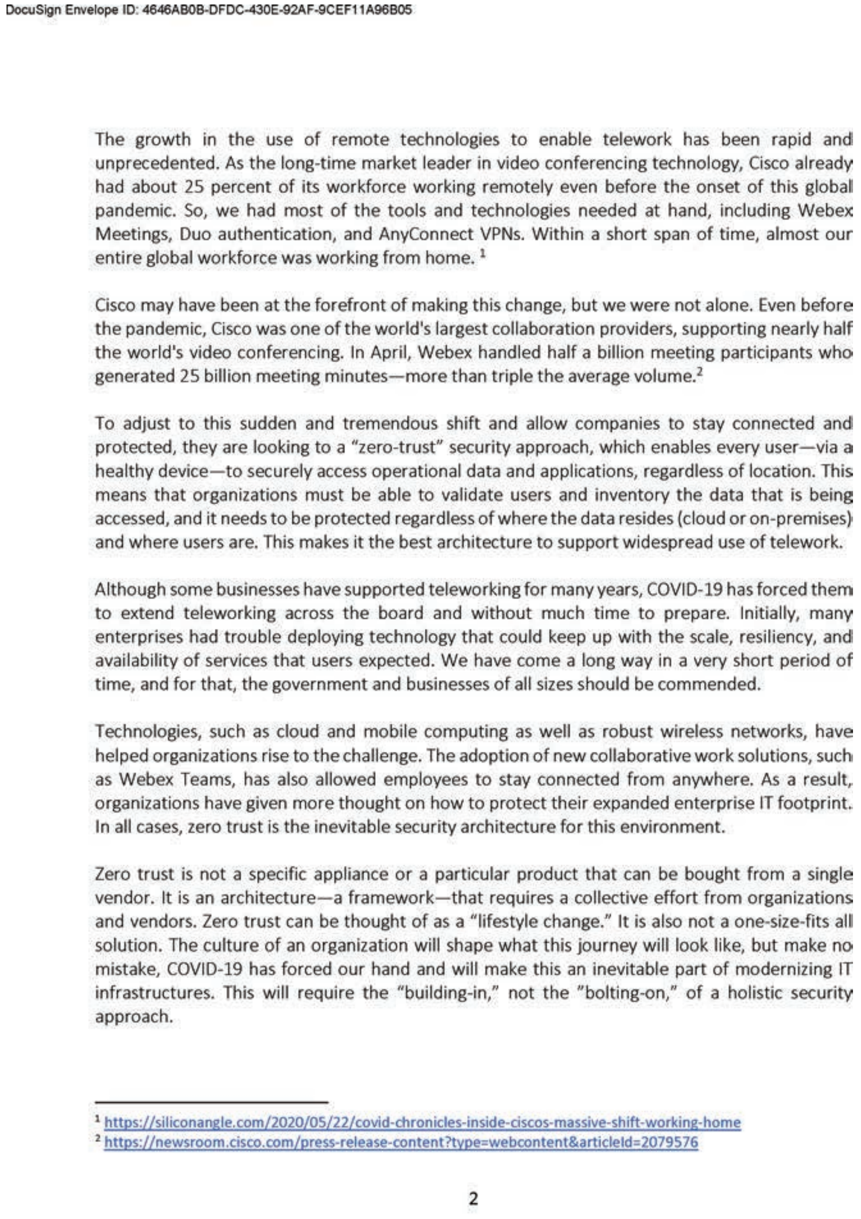
Re: Modernizing Telework: Review of Private Sector Telework Policies during COVID-19 Pandemic

Dear Chairman Lankford and Ranking Member Sinema:

Thank you for your leadership in holding this week's hearing on the rising use of telework in response to the COVID-19 pandemic. I am writing to you on behalf of Cisco Systems, Inc., which acquired Duo Security—an Ann-Arbor, Michigan-based start-up founded in 2009 to provide cloud-based security tools. Cisco's decision to build a portfolio of security services, including those offered by Duo, reflects our recognition that the future relies on ubiquitous access to data and services securely delivered from the cloud. Using these tools, forward-thinking enterprises can build intelligent, adaptable, secure networks that protect sensitive data while enabling remote work. We call this "Zero Trust" networking because it does not make assumptions about security solely based on the location of a user or a device.

While teleworking has long been possible for many roles in both the public and private sector, adoption has lagged over concerns about how to effectively ensure the security of sensitive information and personal data. The rapid spread of the COVID-19 virus in the spring of 2020 forced employers to pivot business operations online to the greatest extent possible. Because their initial focus was understandably on ensuring continuity of operations while maximizing the safety and well-being of customers and employees, decisions often prioritized availability and scalability over data protection and cybersecurity.

Now, several months on, there is a growing realization that some of these hastily adopted changes may be with us for the longer term, or we may require the flexibility to move between different modes of operation to ensure resilience. While there is uncertainty about exactly what the future will bring, we know for sure that the traditional model of a static network with a fixed perimeter has become obsolete in many instances. Organizations can no longer rely on a castle-and-moat security model where all data is accessed from users working within the four walls of their "network." Instead, we must recognize the urgent need to evaluate the security implications of the new normal and make strategic investments that enable business while effectively managing risk of attack by criminal actors and other malfeasants.



The growth in the use of remote technologies to enable telework has been rapid and unprecedented. As the long-time market leader in video conferencing technology, Cisco already had about 25 percent of its workforce working remotely even before the onset of this global pandemic. So, we had most of the tools and technologies needed at hand, including Webex Meetings, Duo authentication, and AnyConnect VPNs. Within a short span of time, almost our entire global workforce was working from home. [1]

Cisco may have been at the forefront of making this change, but we were not alone. Even before the pandemic, Cisco was one of the world's largest collaboration providers, supporting nearly half the world's video conferencing. In April, Webex handled half a billion meeting participants who generated 25 billion meeting minutes—more than triple the average volume.[2]

To adjust to this sudden and tremendous shift and allow companies to stay connected and protected, they are looking to a "zero-trust" security approach, which enables every user—via a healthy device—to securely access operational data and applications, regardless of location. This means that organizations must be able to validate users and inventory the data that is being accessed, and it needs to be protected regardless of where the data resides (cloud or on-premises) and where users are. This makes it the best architecture to support widespread use of telework.

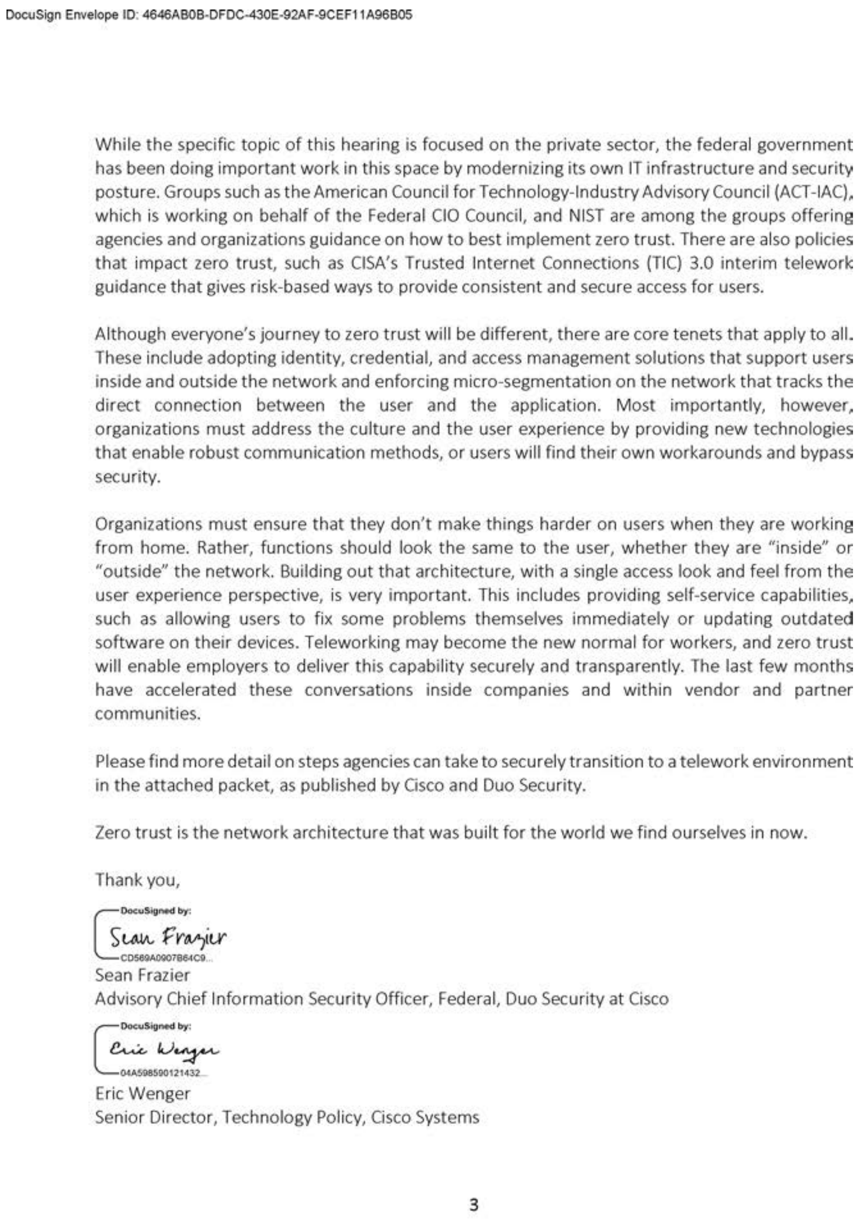
Although some businesses have supported teleworking for many years, COVID-19 has forced them to extend teleworking across the board and without much time to prepare. Initially, many enterprises had trouble deploying technology that could keep up with the scale, resiliency, and availability of services that users expected. We have come a long way in a very short period of time, and for that, the government and businesses of all sizes should be commended.

Technologies, such as cloud and mobile computing as well as robust wireless networks, have helped organizations rise to the challenge. The adoption of new collaborative work solutions, such as Webex Teams, has also allowed employees to stay connected from anywhere. As a result, organizations have given more thought on how to protect their expanded enterprise IT footprint. In all cases, zero trust is the inevitable security architecture for this environment.

Zero trust is not a specific appliance or a particular product that can be bought from a single vendor. It is an architecture—a framework—that requires a collective effort from organizations and vendors. Zero trust can be thought of as a "lifestyle change." It is also not a one-size-fits all solution. The culture of an organization will shape what this journey will look like, but make no mistake, COVID-19 has forced our hand and will make this an inevitable part of modernizing IT infrastructures. This will require the "building-in," not the "bolting-on," of a holistic security approach.

[1] https://siliconangle.com/2020/05/22/covid-chronicles-inside-ciscos-massive-shift-working-home

[2] https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=2079576



While the specific topic of this hearing is focused on the private sector, the federal government has been doing important work in this space by modernizing its own IT infrastructure and security posture. Groups such as the American Council for Technology-Industry Advisory Council (ACT-IAC), which is working on behalf of the Federal CIO Council, and NIST are among the groups offering agencies and organizations guidance on how to best implement zero trust. There are also policies that impact zero trust, such as CISA's Trusted Internet Connections (TIC) 3.0 interim telework guidance that gives risk-based ways to provide consistent and secure access for users.

Although everyone's journey to zero trust will be different, there are core tenets that apply to all. These include adopting identity, credential, and access management solutions that support users inside and outside the network and enforcing micro-segmentation on the network that tracks the direct connection between the user and the application. Most importantly, however, organizations must address the culture and the user experience by providing new technologies that enable robust communication methods, or users will find their own workarounds and bypass security.

Organizations must ensure that they don't make things harder on users when they are working from home. Rather, functions should look the same to the user, whether they are "inside" or "outside" the network. Building out that architecture, with a single access look and feel from the user experience perspective, is very important. This includes providing self-service capabilities, such as allowing users to fix some problems themselves immediately or updating outdated software on their devices. Teleworking may become the new normal for workers, and zero trust will enable employers to deliver this capability securely and transparently. The last few months have accelerated these conversations inside companies and within vendor and partner communities.

Please find more detail on steps agencies can take to securely transition to a telework environment in the attached packet, as published by Cisco and Duo Security.

Zero trust is the network architecture that was built for the world we find ourselves in now.

Thank you,

DocuSigned by:
Sean Frazier
CD569A0907B64C9...
Sean Frazier
Advisory Chief Information Security Officer, Federal, Duo Security at Cisco

DocuSigned by:
Eric Wenger
04A598590121432...
Eric Wenger
Senior Director, Technology Policy, Cisco Systems

Questions for the Record
Senate Homeland Security and Governmental Affairs
"Modernizing Telework: Review of Private Sector Telework Policies during the COVID-19 Pandemic"
Tuesday July 28, 2020
Senator Kyrsten Sinema

**Questions for Mr. Morris**

1. Employees can often find it difficult or intimidating to go to a supervisor with a work-related question. This might especially be true in a fully remote model, where personal interaction and context may be lacking. How have you provided for streamlined vertical communication between supervisors and their employees to ensure productivity?
    - Cultivating trust between supervisors and employees and within teams is critical to ensure a productive, purposeful, and agile working environment – regardless of where work is performed. Virtual environments, though, can make it more difficult to establish and maintain trust. Our point of view is that a flexible and outcome-focused performance management approach is the fundamental vehicle to open lines of communication, collaborate effectively, and continually build mutual trust. When employees know what is expected of them – high quality outcomes rather than just hours logged – they are incentivized to bring issues to light, ask clarifying questions when needed, and generate solutions. The right performance management framework prioritizes regular, meaningful check-ins between employees, supervisors, and teams that provide as close to "real-time" feedback as possible for agile adjustment. This framework then enables the supervisor to collect a data-driven perspective on performance over the course of the review cycle.

2. What training have you implemented for managers and supervisors who are responsible for managing a remote workforce to ensure they are equipped to manage that workforce? How do you measure the success of the training? What training (if any) did you implement for non-supervisory employees?
    - Deloitte teams had been geographically dispersed before the pandemic, so practitioners were already comfortable not working shoulder-to-shoulder next to teammates and supervisors. The firm's flexible culture allowed for a smooth transition from 'work from anywhere' to working just at home. Recent training for employees and supervisors has focused on the technology that is more relevant during fully-remote times, like webinars on Zoom and Microsoft Teams functionality, as well as cyber hygiene learning opportunities (i.e. understanding risks of phishing, at-home printing, etc.). Some of these examples are of systems-specific training, but generally the training that equips our practitioners for this remote working style is embedded in our culture, from hire to retire – a culture that the way we do work is flexible, agile, and outcome (not task) focused. The swift shift to remote work presents an opportunity for government agencies, and all organizations, to consider the value of a culture where employees can feel

comfortable and well-equipped to embrace change, no matter how dramatic or rapid.

Even before the pandemic, our clients have relied on us during times of team transition or change to help them adapt, including the transition to remote management. The tools we use and recommend include immersive "labs" that bring teams and supervisors together to discuss norms, culture, and goals, and ongoing microtrainings to refresh and reinforce those norms, delivered through platforms like Deloitte's FLIP or AI-enabled curated learning systems. In this COVID-19 era, the need for these trainings to be effectively delivered in a virtual environment is critical, and these tools and resources present a fresh approach to the future of learning: flexible learning for flexible workplaces.

3. What should Congress be focusing on now to ensure long-term telework success for both the private and public sector?
   - Our four core learnings emphasize the crucial nature of IT infrastructure & cybersecurity, real estate & location footprint, employee engagement, and performance management in the Respond, Recover, and Thrive framework. To work toward long-term success, we recommend that Congress focus on the following:
     - Looking inward at the government workforce, Congress should reexamine and revitalize its employee engagement and performance management strategies to measure meaningful qualitative and quantitative metrics, while building vertical and horizontal trust.
     - For the country more broadly, Congress should invest in IT infrastructure, like broadband and a reliable hardware and software supply chain, secure collaboration platforms, and cybersecurity guidelines to help corporations and small businesses be well-equipped to handle the challenges of this moment, and accelerate toward the future.

Questions for the Record
Senate Homeland Security and Governmental Affairs
"Modernizing Telework: Review of Private Sector Telework Policies during the COVID-19 Pandemic"
Tuesday July 28, 2020
Senator Kyrsten Sinema

**Questions for Mr. Wilson**

1. Employees can often find it difficult or intimidating to go to a supervisor with a work-related question. This might especially be true in a fully remote model, where personal interaction and context may be lacking. How have you provided for streamlined vertical communication between supervisors and their employees to ensure productivity?

    a. **Our experience is that mutually gratifying work relationships depend upon good communication, either in person or over video or teleconference. Recognizing that there could be some occasions where virtual work makes it more difficult to raise work-related questions, we have proactively encouraged all leaders to utilize our collaboration software for frequent 1:1s to ensure communication occurs as, or more, often than previously.**

2. What training have you implemented for managers and supervisors who are responsible for managing a remote workforce to ensure they are equipped to manage that workforce?

    a. **We hosted weekly leadership meetings and Q&A sessions and provided "tips and tricks" for managing a remotely, including providing articles and case studies.**

    b. How do you measure the success of the training?
    **We measure usage of our collaborative tools. We measure and trend the key capabilities of the tools and group it by department. This data is used to determine if we need to conduct additional training focused on a feature or reach out to the department for more detailed training.**

    c. What training (if any) do you implement for non-supervisory employees?
    **We found that the technology evolves rapidly; therefore, we have implemented multiple approaches to training. The first was to set up an internal web site that contains videos and links to Quick Reference Guides and videos for our collaboration tools. When we initially launched the new technology, we conducted regular weekly live training events that employees could join. We had time at the end for employees to ask questions. And finally, we conduct regular "Tech Thursdays" sessions to provide helpful hints and discuss new features.**

Questions for the Record
Senate Homeland Security and Governmental Affairs
"Modernizing Telework: Review of Private Sector Telework Policies during the COVID-19 Pandemic"
Tuesday July 28, 2020
Senator Kyrsten Sinema

3. What should Congress be focusing on now to ensure long-term telework success for both the private and public sector?

   **At the state level, legislators and regulators often point to the federal government to resolve for poor internet connectivity, competition, or availability, claiming it is a predominantly federal issue. Never before has access and availability of dependable, affordable internet service been more of a basic necessity, for teleworkers as well as tele-learners. Congressional action to promote and ensure dependable internet and cellular service across the country is foundational to long-term telework success.**

   **Likewise, many federal agencies in Washington and across the country have on-site childcare centers. Access to dependable and affordable childcare is a critical component to long-term telework success, just as it is for full-time, in-office workers. Having safe and affordable childcare options for working families helps all workers succeed.**

4. Social interaction in the workplace is not only helpful for professional development, but also in cementing the relationships inherent in creating a team. What steps have you taken to ensure your employees continue to feel fulfilled and supported while teleworking and have you discovered any tools available to help employers enhance and maintain workforce camaraderie?

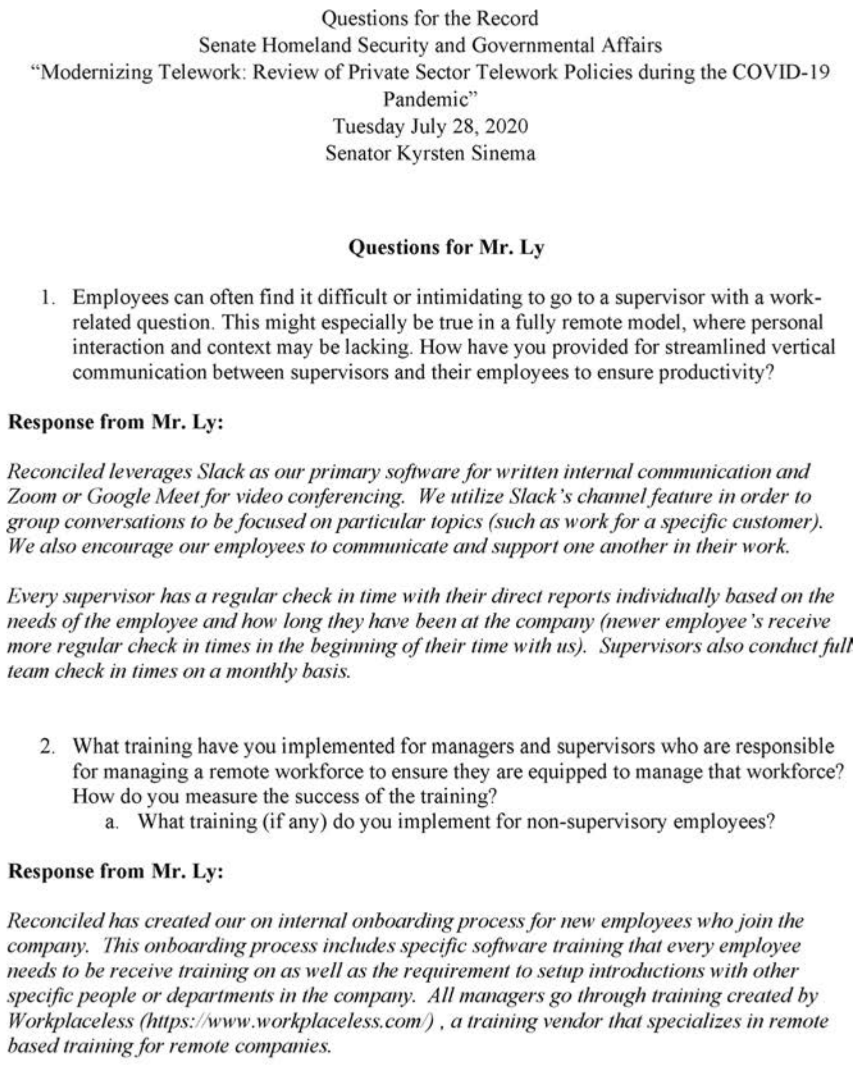
   a. As a follow-up on this topic, are there specific actions you would recommend a company take regarding telework during a pandemic when feelings of fear and social isolation are exacerbated?

      i. **We encourage frequent check-ins via phone and video, the use of recorded video messaging, surveys of our leaders.**
      ii. **Many of our leaders host virtual happy hours or other virtual gatherings.**
      iii. **We monitor the use of our collaboration software and believe our supervisors are remaining "in touch" with their teams.**

Questions for the Record
Senate Homeland Security and Governmental Affairs
"Modernizing Telework: Review of Private Sector Telework Policies during the COVID-19 Pandemic"
Tuesday July 28, 2020
Senator Kyrsten Sinema

5. One of the greatest challenges with telework during the pandemic is the continued closure of most schools. Parents have to manage their children's education needs while also juggling their own work responsibilities. This requires great flexibility on the part of companies and families. What recommendations do you have for companies, or families, on how to set up or expand a telework plan so people can be both a good parent and a good worker?

    a. **Williams has fostered an open-communication and flexible environment during these difficult times. As a company, we have allowed employees to elect a remote work option through December 2020 to manage childcare or other family demands. Many of our teams are able to self-organize and find models that allow them to support work needs based on the team's individual challenges. We encourage our managers to be flexible and understanding of the potential distractions that childcare and ever-changing school schedules present and to remain in touch with families who have those challenges.**



Questions for the Record
Senate Homeland Security and Governmental Affairs
"Modernizing Telework: Review of Private Sector Telework Policies during the COVID-19 Pandemic"
Tuesday July 28, 2020
Senator Kyrsten Sinema

**Questions for Mr. Ly**

1. Employees can often find it difficult or intimidating to go to a supervisor with a work-related question. This might especially be true in a fully remote model, where personal interaction and context may be lacking. How have you provided for streamlined vertical communication between supervisors and their employees to ensure productivity?

**Response from Mr. Ly:**

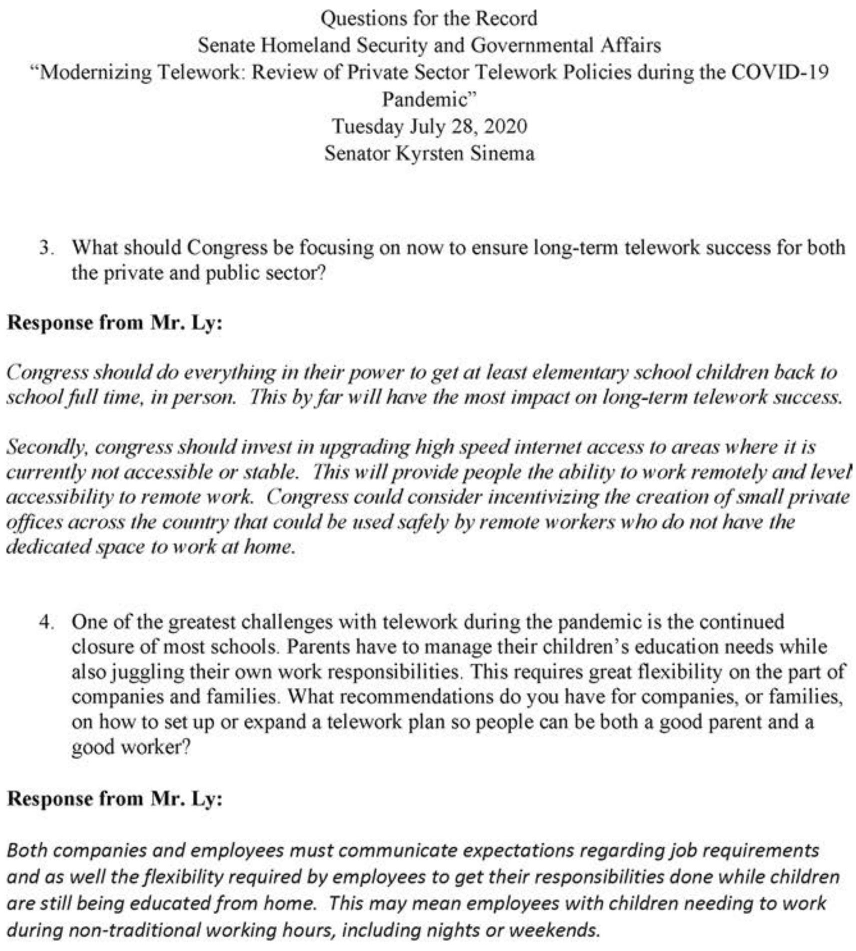
*Reconciled leverages Slack as our primary software for written internal communication and Zoom or Google Meet for video conferencing. We utilize Slack's channel feature in order to group conversations to be focused on particular topics (such as work for a specific customer). We also encourage our employees to communicate and support one another in their work.*

*Every supervisor has a regular check in time with their direct reports individually based on the needs of the employee and how long they have been at the company (newer employee's receive more regular check in times in the beginning of their time with us). Supervisors also conduct full team check in times on a monthly basis.*

2. What training have you implemented for managers and supervisors who are responsible for managing a remote workforce to ensure they are equipped to manage that workforce? How do you measure the success of the training?
    a. What training (if any) do you implement for non-supervisory employees?

**Response from Mr. Ly:**

*Reconciled has created our on internal onboarding process for new employees who join the company. This onboarding process includes specific software training that every employee needs to be receive training on as well as the requirement to setup introductions with other specific people or departments in the company. All managers go through training created by Workplaceless (https://www.workplaceless.com/) , a training vendor that specializes in remote based training for remote companies.*



Questions for the Record<br>
Senate Homeland Security and Governmental Affairs<br>
"Modernizing Telework: Review of Private Sector Telework Policies during the COVID-19 Pandemic"<br>
Tuesday July 28, 2020<br>
Senator Kyrsten Sinema

3. What should Congress be focusing on now to ensure long-term telework success for both the private and public sector?

**Response from Mr. Ly:**

*Congress should do everything in their power to get at least elementary school children back to school full time, in person. This by far will have the most impact on long-term telework success.*

*Secondly, congress should invest in upgrading high speed internet access to areas where it is currently not accessible or stable. This will provide people the ability to work remotely and level accessibility to remote work. Congress could consider incentivizing the creation of small private offices across the country that could be used safely by remote workers who do not have the dedicated space to work at home.*

4. One of the greatest challenges with telework during the pandemic is the continued closure of most schools. Parents have to manage their children's education needs while also juggling their own work responsibilities. This requires great flexibility on the part of companies and families. What recommendations do you have for companies, or families, on how to set up or expand a telework plan so people can be both a good parent and a good worker?

**Response from Mr. Ly:**

*Both companies and employees must communicate expectations regarding job requirements and as well the flexibility required by employees to get their responsibilities done while children are still being educated from home. This may mean employees with children needing to work during non-traditional working hours, including nights or weekends.*

Questions for the Record
Senate Homeland Security and Governmental Affairs
"Modernizing Telework: Review of Private Sector Telework Policies during the COVID-19 Pandemic"
Tuesday July 28, 2020
Senator Kyrsten Sinema

**Questions for Mr. John Zanni, CEO, Acronis SCS**

1. **Employees can often find it difficult or intimidating to go to a supervisor with a work-related question. This might especially be true in a fully remote model, where personal interaction and context may be lacking. How have you provided for streamlined vertical communication between supervisors and their employees to ensure productivity?**

As CEO, it is my duty to ensure the productivity and wellbeing of my workforce, no matter the circumstances. While COVID-19 has added a new dimension to the challenges of understanding and addressing employee concerns or productivity blockers, Acronis SCS has used our shift to remote work as a welcome opportunity to engage with employees in new and creative ways.

The first is the introduction of daily departmental stand up syncs. These short virtual meetings help supervisors and their teams stay aligned on ongoing tasks and strategic priorities, while personalizing remote interactions. We also conduct monthly town halls, where both I and my HR team provide updates to employees on company progress and the various resources available to them. Each of these town halls ends with an open Q&A period, where employees are free to bring up any concerns or questions they may have. I also require my leadership team to conduct weekly virtual one-on-one meetings with each of their direct reports.

Though we already had internal instant messaging and task manager applications in place prior to the pandemic, I've encouraged my leadership team to use these applications more frequently to provide clear channels of communication both vertically and horizontally. I've also encouraged my leadership team to implement strategies they know will work best for their employees. For example, one of my directors keeps a Zoom meeting open all day, so his employees can hop on or off as needed to discuss and resolve issues in real time.

Another way we've helped streamline vertical communication is our introduction of anonymous employee surveys that help identify pain points and productivity blockers in a non-intimidating setting. These survey have allowed us to not only identify physical needs (like high speed internet and office equipment stipends), but mental/emotional stressors as well (like the need for more flexible work hours for employees balancing children's at-home learning and the ability to 'work from anywhere' in the United States to allow for family visits).

The above efforts have allowed our company to quickly address any employee needs and concerns as they arise, while maintaining (and, in many cases, exceeding) our pre-COVID-19 productivity expectations.

Questions for the Record
Senate Homeland Security and Governmental Affairs
"Modernizing Telework: Review of Private Sector Telework Policies during the COVID-19 Pandemic"
Tuesday July 28, 2020
Senator Kyrsten Sinema

2. **What training have you implemented for managers and supervisors who are responsible for managing a remote workforce to ensure they are equipped to manage that workforce? How do you measure the success of the training?**

    a. **What training (if any) do you implement for non-supervisory employees?**

In addition to the efforts described above that have helped supervisors more effectively manage their remote workforces, my HR team has offered a variety of training opportunities to both supervisors and their employees. Topics range from "how to adapt to a remote environment" to "how to present your best self in a Zoom meeting." We measure the success of these efforts and collect suggestions for additional training topics and morale-boosting activities through our anonymous employee surveys. We have also tailored our regular, mandatory employee cybersecurity trainings to address remote work vulnerabilities and safety.

Another way we've aided management and productivity during this work-from-home period is our adoption of a new system for evaluating employees' quarterly performance. The system provides supervisors the opportunity to develop clear goals in collaboration with each employee at the start of each quarter, ensuring performance is measured in a transparent fashion and all parties have ownership in the process. Managers are encouraged to check in with employees throughout the quarter to assess any roadblocks preventing them from reaching their stated goals.

3. **From a cybersecurity lens, what lessons regarding how the federal government and Congress advances cyber protection policies and actions can be learned from the private sector's transition to telework?**

The most critical piece of advice I can offer to the federal government and Congress as they navigate the challenges of remote work (and consider added remote work flexibility for certain roles/agencies in the future) is ensuring cyber protection remains a focal point of the conversation and planning process. The stakes are simply too high and the potential consequences too great to do otherwise.

Having a layered "defense in depth" approach in place was essential to Acronis SCS' successful transition to remote work. Though the specifics of such an approach will look different depending on the needs of a given organization, adopting frameworks centered on zero trust and least privilege access are key places for the public sector to start. That way, when a cyberattack hits (an inevitability at one point or another under normal circumstances, let alone when employees are teleworking), its impact is contained, and critical services remain operational.

Another lesson the public sector can glean from private sector telework transitions is balanced consideration of the five vectors of cyber protection: safety, accessibility, privacy, authenticity, and security. Far too often, these five vectors are pitted against one another in a zero-sum game, but they need not be mutually exclusive. In fact, when balanced appropriately, they are the key to keeping the organizations both protected and productive, whether employees are teleworking or in office.

**Safety:** Being physically "safe" means avoiding things that can cause injury, pain, and loss. The same is true for ensuring digital safety. Creating reliable backups of data, applications, and systems – and storing them where they cannot be compromised – is the most future-proof way to keep everything safe.

**Accessibility:** In today's mobile world, individuals carry more computing power in their pockets than was used to send a man to the moon. To harness that technological advancement, public sector organizations need to be able to access data, applications, and systems from any location and at any time. Implementing a cyber protection framework ensures that access, while balancing it against the need to keep digital environments and assets safe, private, authentic, and secure.

**Privacy:** From accidental data leaks to targeted espionage, keeping things private is a tricky but essential need across the public sector. Yet upticks in breaches and ransomware attacks show too few organizations are taking appropriate steps to combat modern threats. Managing who can view and use sensitive data, applications, and systems should be under tight control – whether that means limiting user permissions or employing enterprise-grade encryption to shield sensitive information from prying eyes.

**Authenticity:** For any organization's IT personnel, being able to know and trust that backups are authentic is absolutely vital, since recovering a file, server, or entire infrastructure from an altered or corrupted version can put ALL users, devices, and materials at risk. Given the threat posed by unauthorized alterations, public sector IT teams need a way to validate a backup's authenticity before relying on it for recovery. One such method is blockchain notarization, which ensures a file has not been tampered with or altered.

**Security:** At its most basic level, security means freedom from danger. Unfortunately, the digital world is filled with constantly evolving dangers – from sophisticated ransomware that encrypts files to cryptomining malware that hijacks system resources while injecting other threats. Securing the public sector's computing environments, whether those environments involve telework endpoints or not, requires a protection strategy that stops all digital threats, including both known and previously unknown, or zero day, vulnerabilities.

Effectively balancing these vectors can often seem like a daunting task, particularly for resource-strapped organizations. But the US public sector need not navigate this challenge alone. There are solutions already on the market designed to help public sector organizations of all shapes and sizes integrate these practices, so their critical data, applications, and systems stay protected, no matter what – not just against the latest cyber threat du jour, but well into the future.

Questions for the Record
Senate Homeland Security and Governmental Affairs
"Modernizing Telework: Review of Private Sector Telework Policies during the COVID-19 Pandemic"
Tuesday July 28, 2020
Senator Kyrsten Sinema

4. **What should Congress be focusing on now to ensure long-term telework success for both the private and public sector?**

Two factors are critical for ensuring long-term telework success and digital resilience. The first is training – not just the training of individual employees as human firewalls for their organizations while they work from home, but the large-scale training and reskilling of American workers to address our nation's critical shortage of cyber and IT talent. As of May 2020, there were more than 500,000 open cybersecurity jobs across the United States. More than 30,000 of those openings were within public sector institutions. With such a shortfall of personnel, it comes as little shock that thirty-six percent of public sector organizations admit to sacrificing mobile security to "get the job done."

The perennial struggle to find cyber talent has been further amplified by COVID-19, which spurred a sixty-five percent surge in overall US demand for information security personnel. As all organizations, both public and private, navigate remote work realities and seek to better protect themselves against related cyber threats, Congress should support and fund efforts that expand America's pool of qualified cyber talent.

The second critical area Congress should focus its efforts is on providing funding to help state and local governments address cybersecurity shortfalls. In 2018, less than half of American states had a separate budget line item dedicated to cybersecurity. Budgetary pressures from COVID-19 and related recovery efforts have constricted cybersecurity spends even more at a time when they are arguably more essential than ever before. Access to grants and conditional funding opportunities, like those outlined in the State and Local IT Modernization and Cybersecurity Act (H.R.8048), will help state and local governments keep cybersecurity top of mind amidst a sea of competing priorities.

○