TESTIMONY OF

Dr. Diana L. Burley

Vice Provost for Research
Professor, Public Administration and Policy
Professor, Information Technology and Analytics
American University
Washington, DC

BEFORE THE

United States House of Representatives Committee on Science, Space & Technology
Subcommittee on Space and Aeronautics

HEARING ON

Cybersecurity at Nasa:
Ongoing Challenges and Emerging Issues for Increased Telework During Covid-19

September 18, 2020

Online via Video Conferencing

Subcommittee Chairwoman Horn, Ranking member Babin, and distinguished Members of the Committee, thank you for the opportunity to appear before you today. As the nation continues to navigate the complex and uncertain environment of the global pandemic, it is vital that we engage in a robust discussion on the cybersecurity related challenges and emerging issues for increased telework during COVID-19. I appreciate the Committee's commitment to exploring these issues and trust that my remarks today will enhance our collective efforts to safeguard the American people.

My name is Dr. Diana L. Burley. I am vice provost for research at American University (AU) where I am also professor of public administration and policy in the School of Public Affairs and professor of information technology & analytics in the Kogod School of Business. American University researchers develop innovative, impactful, and game-changing solutions to the world's most pressing problems. Guided by our strategic plan, Changemakers for a Changing World, we empower graduates to navigate, shape and lead the future of work. Through the lens of our Changemakers strategy, AU researchers are pushing the boundaries of discovery in health care, data science, social equity and security. In my remarks today, I will highlight how the interplay of these areas support the development of a holistic strategy to address cybersecurity issues surrounding the exponential growth in telework during this unprecedented time.

First, a disclaimer – today I will provide testimony as a private citizen and my views do not represent the official position of American University or any other institution to which I have an affiliation.

My views are shaped by a decades long career leading cybersecurity workforce development initiatives, defining best practices in cybersecurity awareness and education programs, developing strategies to strengthen organizational cybersecurity posture, and informing global cybersecurity policy and practice. I have authored nearly 100 publications on cybersecurity and IT-enabled change. I am a member of the US National Academies of Science, Engineering and Medicine Board on Human-Systems Integration, the Education Council of the Association for Computing Machinery, and an affiliated researcher with the Johns Hopkins University Applied Physics Laboratory. My prior roles have included executive director of the Institute for Information Infrastructure Protection (I3P) and lead program director for the federal Scholarship for Service Cyber Corps program. Notably, the impact of my efforts has been recognized by a range of honors including; SC Magazine Eight Women in IT Security to Watch, a woman of influence by the Executive Women's Forum in Information Security, Risk Management and Privacy, cybersecurity educator of the year, government leader of the year, and a top influencer in information security careers. In short, my experiences across academia, government, and industry provide me with a unique vantage point from which to offer the Committee insight on the subject of this hearing.

Telework During COVID-19

Concerns over exposure to COVID-19 have accelerated a mass migration to virtual settings. While teleworking arrangements have existed for years, never before have we seen the range and volume of remote workers or remote working environments. Employees across the spectrum of demographic categories and technical abilities are now working remotely and engaging with their employers, colleagues and customers through a digital interface and on a range of devices. Securing this activity necessitates that we recognize both the technical needs and the environmental factors that shape user behavior.

Consider the following –

Novice users and novice experiences create vulnerabilities. In the hurried transition to remote work, agencies did not have sufficient time to prepare novice users for the complexities of their newly virtual working environments. Technical capabilities, hardware and software requirements for remote access, were largely the focus of these initial transitional efforts. However, not only does remote work often offer fewer protections, but overall security also is more reliant upon individual decisions by employees and non-employees alike. Even seasoned users, who have developed behaviors in accordance with on-site protections, face new challenges and can find themselves less prepared to avoid the vulnerabilities exposed by their remote working environments.

Employees are working under duress. COVID-19 continues to drive economic instability, health related concerns, anxiety, and confusion. These fears are exacerbated by weather-related disasters, a country divided over racial injustice, and a strained political climate. Employees are worried about meeting their basic needs – safety, food, shelter and health, and are less likely to attend to seemingly less important priorities like cybersecurity.

Cyber criminals exploit targets of opportunity. Everyday more activities move online – people are teleworking, engaging with social networks, learning and shopping. Unfortunately, this shift in activity provides a larger attack surface and leads to more opportunities for cyber criminals. Social engineering methods using fraud, misdirection, and dis-information are all designed to exploit vulnerabilities.

To combat these types of attacks, agencies can adapt cyber awareness campaigns to account for environmental changes and establish strong protocols for robust cyber hygiene practices outside of the workplace. Basic cyber hygiene guidance such as – don't click on links from unknown senders, use strong and unique passwords, set multi-factor authentication, and keep virus protection software up to date, all can make a significant difference.

Users bring their entire selves online. If we use the public health analogy of "treating the whole patient" we can strengthen the efficacy of guidance to engage in robust cyber hygiene activities during COVID-19. In public health practice, successful treatment is inextricably linked to the social and environmental conditions of the patients. Treatment outcomes are the result

of a complex interplay of comorbidities. Today, in the midst of the COVID-19 pandemic, we must recognize that while basic cyber hygiene practice is relatively doable under normal circumstances, these are not normal times. The global pandemic has caused a heightened sense of uncertainty about every facet of life. In the face of this reality, we must be keenly aware that our workers are distracted, frightened, and fatigued. This is especially true for the most vulnerable users. As such, strategies to strengthen the cybersecurity of teleworkers must consider the full spectrum of user experiences and address the complex realities of their needs.

Summary

The points outlined above represent a snapshot of the benefit of using a holistic approach to reduce the impact of cybersecurity related vulnerabilities. I have long advocated for this type of approach. Now, and with a greater sense of urgency, we must collaboratively develop interventions that address the dynamic interplay between technical and environmental variables that shape the true cybersecurity posture across the broad range of teleworkers as they navigate the COVID-19 environment.

At American University, we stand ready to support the nation and the evolution of policy and practice by examining the complex relationship between health care, data science, social equity, and security. I look forward to continued engagement with this esteemed Committee to develop concrete strategies to raise awareness of the threat, encourage actions that increase the cybersecurity of the nation's employees, and protect our most vulnerable citizens. Working together, we can prevent the addition of a cybersecurity crisis to this list of COVID-19 related tragedies facing our nation.

Thank you.