Government Business Council **Flash Poll**

Underwritten by DUO

Securing the Expanding Perimeter

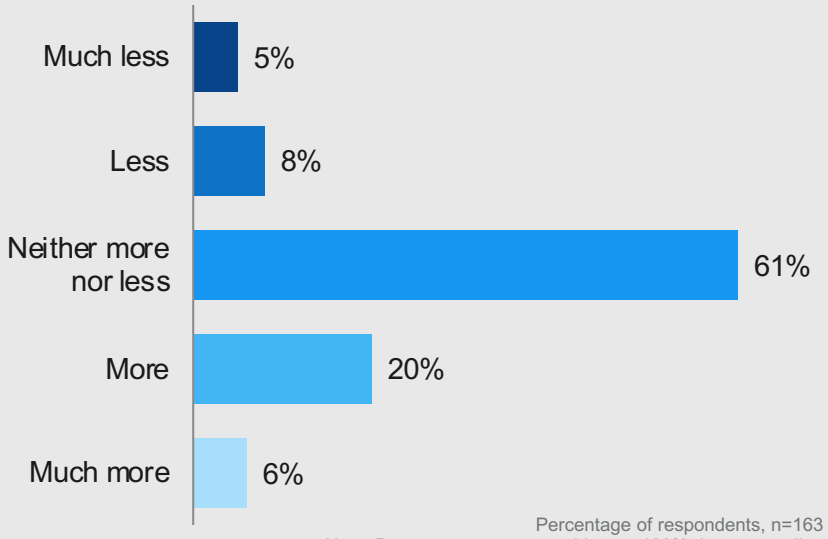
A Flash Assessment of Federal Employee Security Practices and Perceptions

Introduction

After OMB called for maximal telework in March of 2020, agencies moved quickly: the Department of Defense activated 900,000 remote user accounts,[1] the National Science Foundation shifted 100% of its workforce to telework,[2] and the State Department equipped 107,000 of its global officers with remote capabilities.[3] The shift to remote work preserved efficiency, but did it open the door for cyber vulnerabilities? Government Business Council (GBC) polled federal employees in June to find out.

At least 1 in 4 believe that their organization's network is more vulnerable while remote

"My organization's network is _____ vulnerable now that most of our workforce is remote."



Percentage of respondents, n=163
Note: Percentages may not add up to 100% due to rounding

- **61%** of federal respondents say that their network security is neither more nor less vulnerable than before maximal telework.
- **13%** say that their network has become less vulnerable while a large portion of the workforce is at home.

"We do have new concerns about cybersecurity because now devices are either in an uncontrolled space, or we're allowing people to use cloud-based resources for business, but it's through a personal computer that we don't really have visibility into."

Michael Mestrovich, Deputy CIO, State Department, July 9, 2020[3]

Duo's Perspective

At Duo, we want agencies to worry about their mission, not cybersecurity.[1] This objective has never been more pertinent than at this moment, as the government carries out critical services for a country in crisis. Our modern access security is designed to safeguard all users, devices, and applications, so that government employees can focus on what they do best.

At least 1 in 4 government employees GBC surveyed said that their network is more vulnerable while the workforce is remote, which is a strong indication that agency networks may not yet be adapted to the "new normal." Duo is here to enable an increasingly remote workforce with confidence. Our security solutions complement any technical environment, and they're engineered to verify identity and establish device trust no matter how, where, or when your users choose to log in.

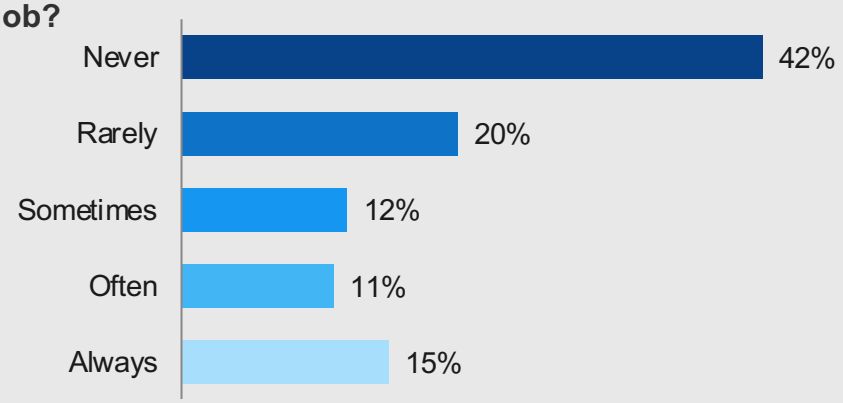
Government Business Council **Flash Poll**

Underwritten by

DUO

58% use their personal devices for work-related tasks to some extent

How often do you use your personal device to do your job?



Percentage of respondents, n=158
Note: Percentages may not add up to 100% due to rounding

- **Over a quarter** use their personal device *often* or *always*.

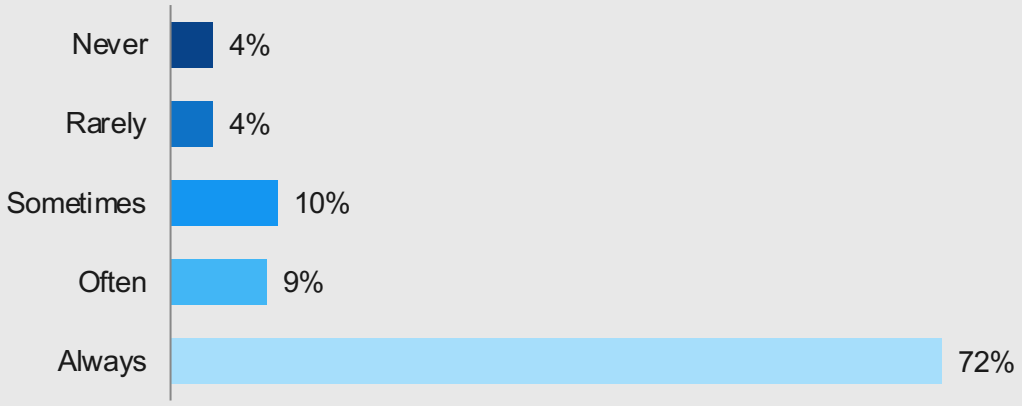
The history of Bring Your Own Device (BYOD) policies in the government is wrought with security vulnerabilities.

In September 2019, audit of the IRS' BYOD policy, with more than 1,200 program users, exposed significant data leakage, citing 68 critical and high-risk vulnerabilities in just one month., 18 of which were easily exploitable, including iPhone screenshot capabilities.[4]

Promisingly, 72% always use two-step authentication…but what about the other 28%?

- **8%** never or rarely use two step authentication, making themselves vulnerable to cyber threats.
- **Almost 20%** use two step identity verification sometimes or often. Increasing adoption within this group is feasible and would reduce a large portion of end-user vulnerabilities.

"When I sign into a device to access work applications, I _____ complete two steps to verify my identity."



Percentage of respondents, n=158
Note: Percentages may not add up to 100% due to rounding

Methodology
GBC fielded a 3-question poll on mobile device security to a random sample of 163 federal employees in May 2020.

Sources

1. Department of Defense: "Growth in DoD Telework Capabilities May Outlive Coronavirus Pandemic." April 13, 2020. https://www.defense.gov/Explore/News/Article/Article/2147123/dod-officials-brief-media-on-covid-19-efforts/
2. Meritalk: "NSF Cruising Along with 100 Percent of Staff Teleworking." April 17, 2020.. https://www.meritalk.com/articles/nsf-cruising-along-with-100-percent-of-staff-teleworking/
3. Meritalk: "CIO Crossroads: Federal IT in COVID Crisis- State Department Edition." July 9, 2020. https://www.meritalk.com/articles/cio-crossroads-federal-it-in-the-covid-crisis-state-department-edition/
4. Treasury Inspector General For Tax Administration: "The Bring Your Own Device Program's Security Controls Need Improvement." September 12, 2019. https://www.treasury.gov/tigta/auditreports/2019reports/201920046fr.pdf3

About Government Business Council
As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of *Government Executive*'s 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

About Duo:
Duo's secure access solutions help you reduce risk and prepare for the future. Federal agencies and government can modernize your IT environments and start your zero-trust journey. Duo democratizes security to secure democracy and relieve the pain points and challenges of federal IT modernization initiatives. Learn more at https://duo.com/use-cases/industry-solutions/federal-government.