Intergovernmental Audit Forum

23rd Biennial Forum of Government Auditors

Deborah Snyder, MBA, GCIS, GSTRT, CISSP, CRISC, PMP

Cyber Strategist, Senior Fellow - Center for Digital Government, FMR. State CISO

Thomas Rohrbach, Branch Chief, DHS OIG

Information Assurance and Testing for Technology Audits and Analytics Support

Nicholas Marinos, GAO, Director, Information Technology and Cybersecurity

Intergovernmental Audit Forum

23rd Biennial Forum of Government Auditors

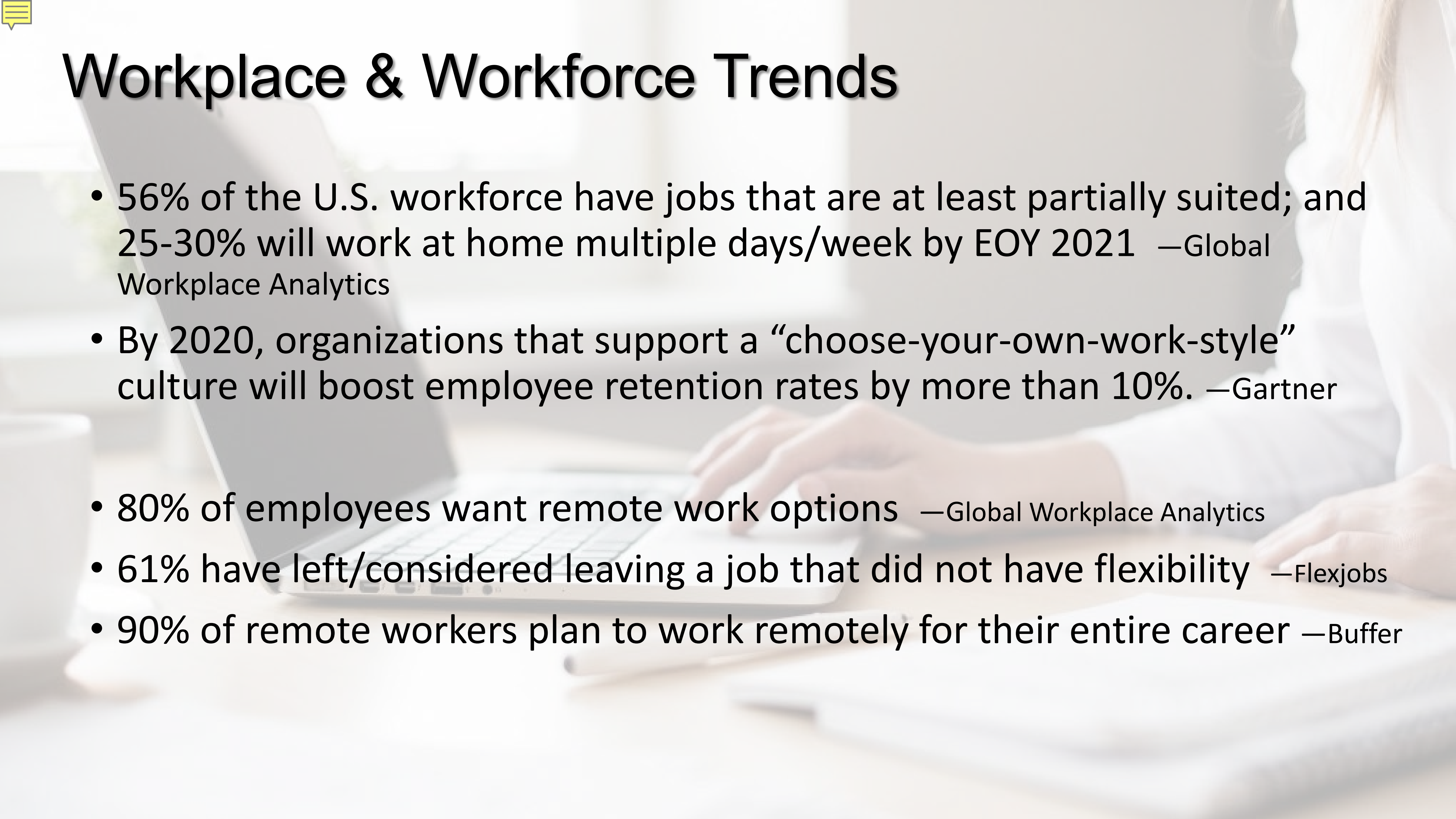
Deborah Snyder, MBA, GCIS, GSTRT, CISSP, CRISC, PMP

Cyber Strategist, Senior Fellow - Center for Digital Government,
FMR. State CISO

The 21st Century Workplace

- We live in a globally-connected world
- Business is rapidly transforming
  - Digital
  - Cloud
  - Mobile
  - Automation
  - Personalized delivery
  - 24x7 access – any form
- Workplace & workforce dynamics are shifting
  - Innovation first, automate as much as possible
  - Leverage enabling tools & technologies
  - Adapt swiftly
  - Work-From-Anywhere mindset

Workplace & Workforce Trends



- 56% of the U.S. workforce have jobs that are at least partially suited; and 25-30% will work at home multiple days/week by EOY 2021 —Global Workplace Analytics
- By 2020, organizations that support a “choose-your-own-work-style” culture will boost employee retention rates by more than 10%. —Gartner
- 80% of employees want remote work options —Global Workplace Analytics
- 61% have left/considered leaving a job that did not have flexibility —Flexjobs
- 90% of remote workers plan to work remotely for their entire career —Buffer

Challenges & Concerns

- Rapid shift to remote work
- Connectivity, collaboration, communication tools
- Secure remote access - strong authentication, trust, end-to-end monitoring and protection
- Business impact / continuity of operations
- Scalability, capacity & infrastructure limitations
- Increased risk, cyber threats
- Resource constraints
- 3rd party risk management – supply chain dependencies, security

Cyber Hygiene “Basics”

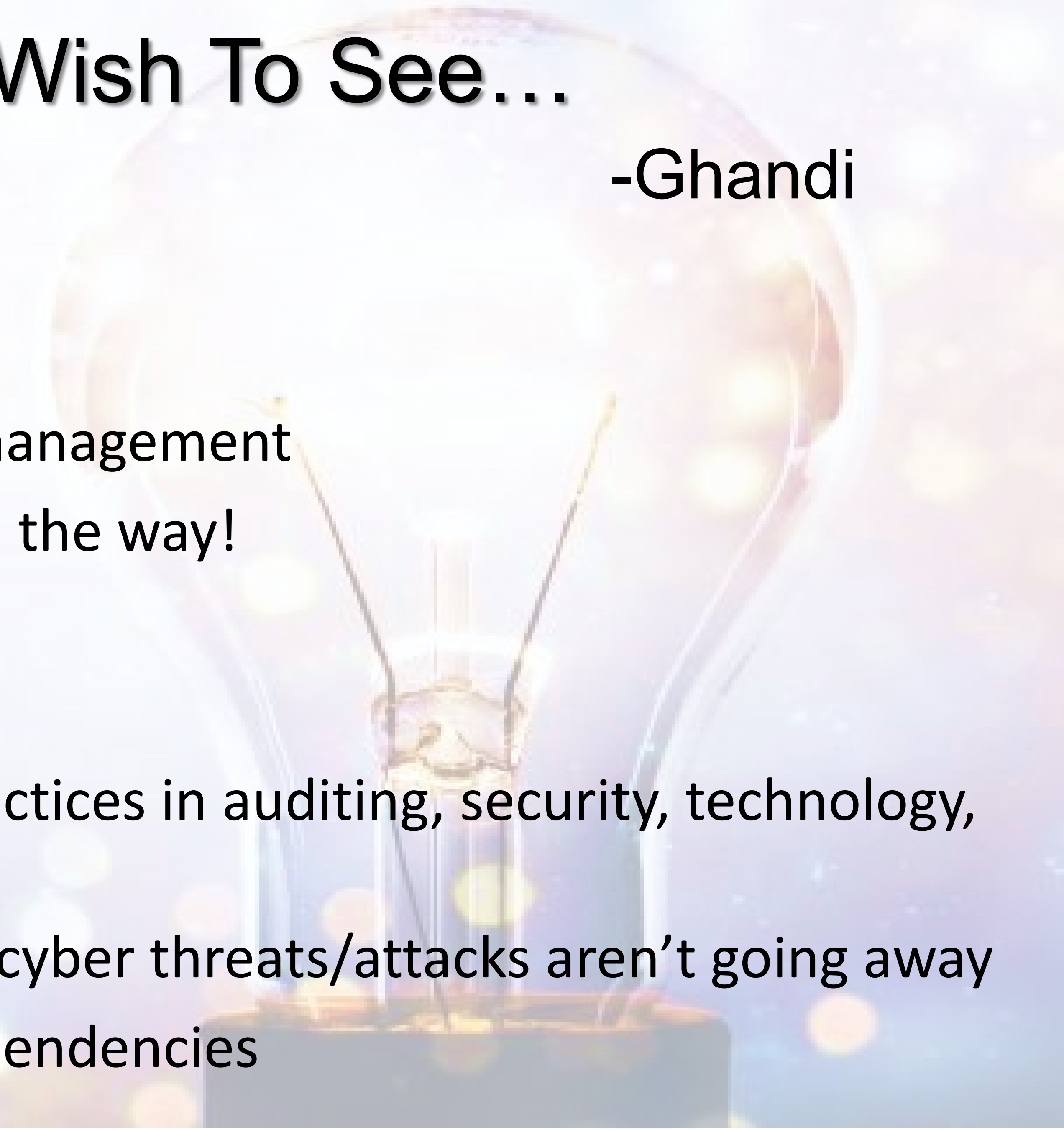
- Train employees - awareness & education
- Take stock - inventory critical systems/software
- Keep systems up-to-date - secure configurations, patching
- Data protection – classification, encryption of sensitive data
- Strong authentication - manage accounts & access
- Backup & data recovery – 3-2-1; testing/validation
- Proactive defenses – email, Internet, data loss prevention
- Continuous monitoring & detection
- Secure System Development Life Cycle (build & buy)
- Preparedness – incident reporting, response, exercises

Be The Change You Wish To See…

-Ghandi

- Re-image your practices
- Future-proof your workforce
- Balance innovation with risk management
- Model desired practices – lead the way!
- Incorporate mindfulness

- Do the “Basics” well – best practices in auditing, security, technology, automation, policy
- Preparedness and resiliency – cyber threats/attacks aren’t going away
- Understand 3rd-party risk/dependencies



Intergovernmental Audit Forum

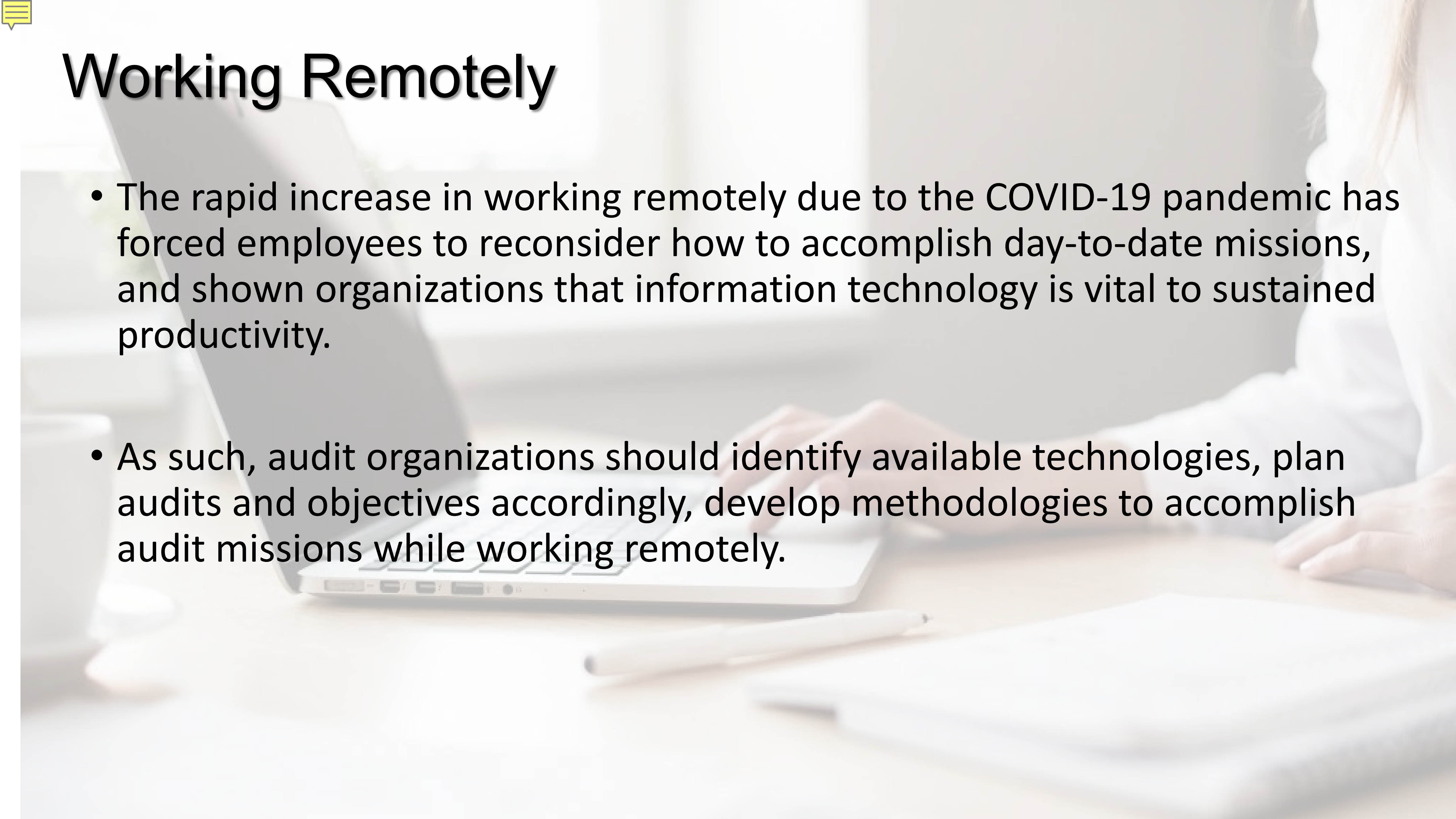
23rd Biennial Forum of Government Auditors

Auditing remotely and ensuring security of data and information (i.e., Cybersecurity)

Thomas Rohrback, Branch Chief, DHS OIG

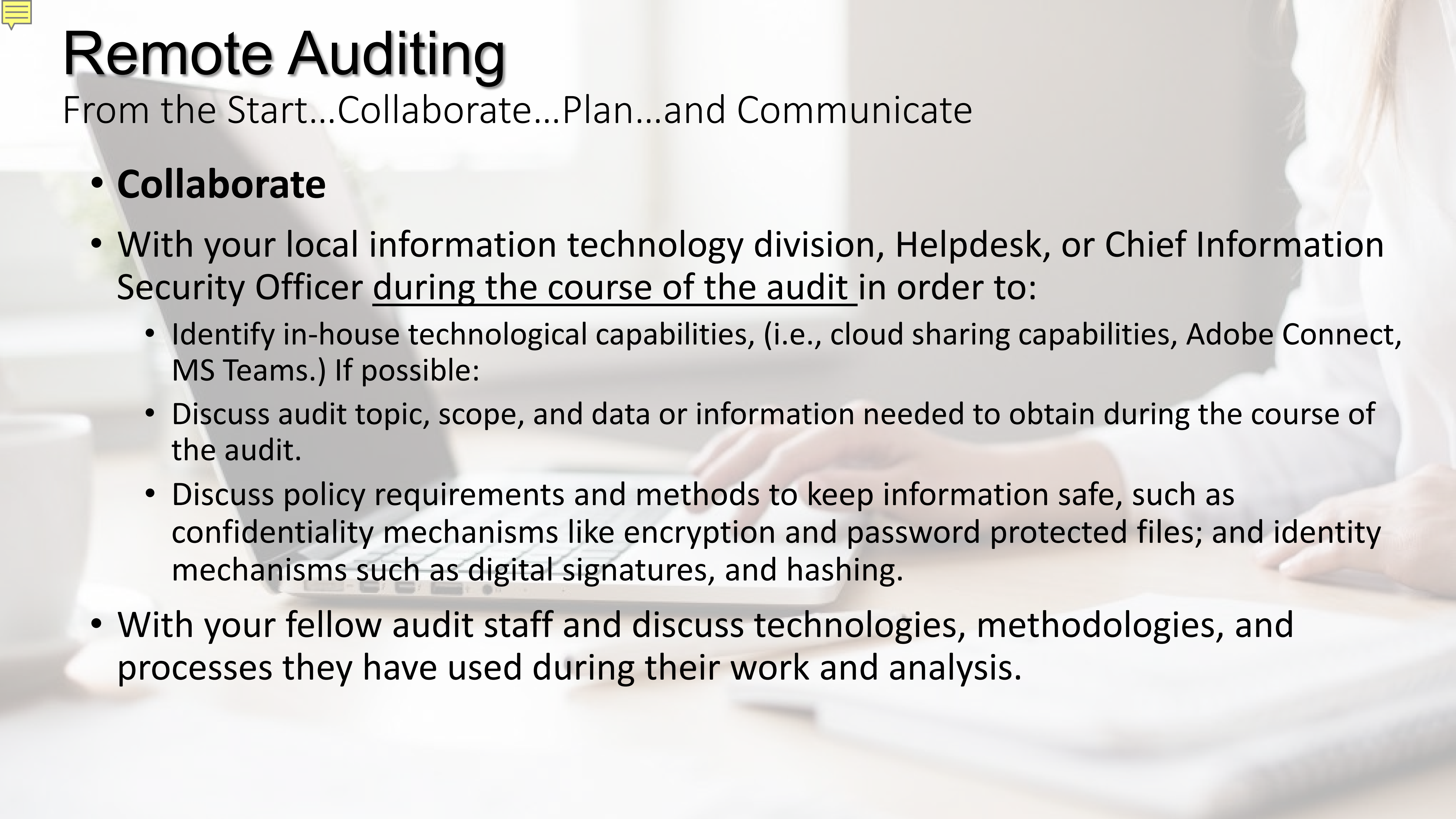
Information Assurance and Testing for Technology Audits and Analytics Support

Working Remotely



- The rapid increase in working remotely due to the COVID-19 pandemic has forced employees to reconsider how to accomplish day-to-date missions, and shown organizations that information technology is vital to sustained productivity.

- As such, audit organizations should identify available technologies, plan audits and objectives accordingly, develop methodologies to accomplish audit missions while working remotely.



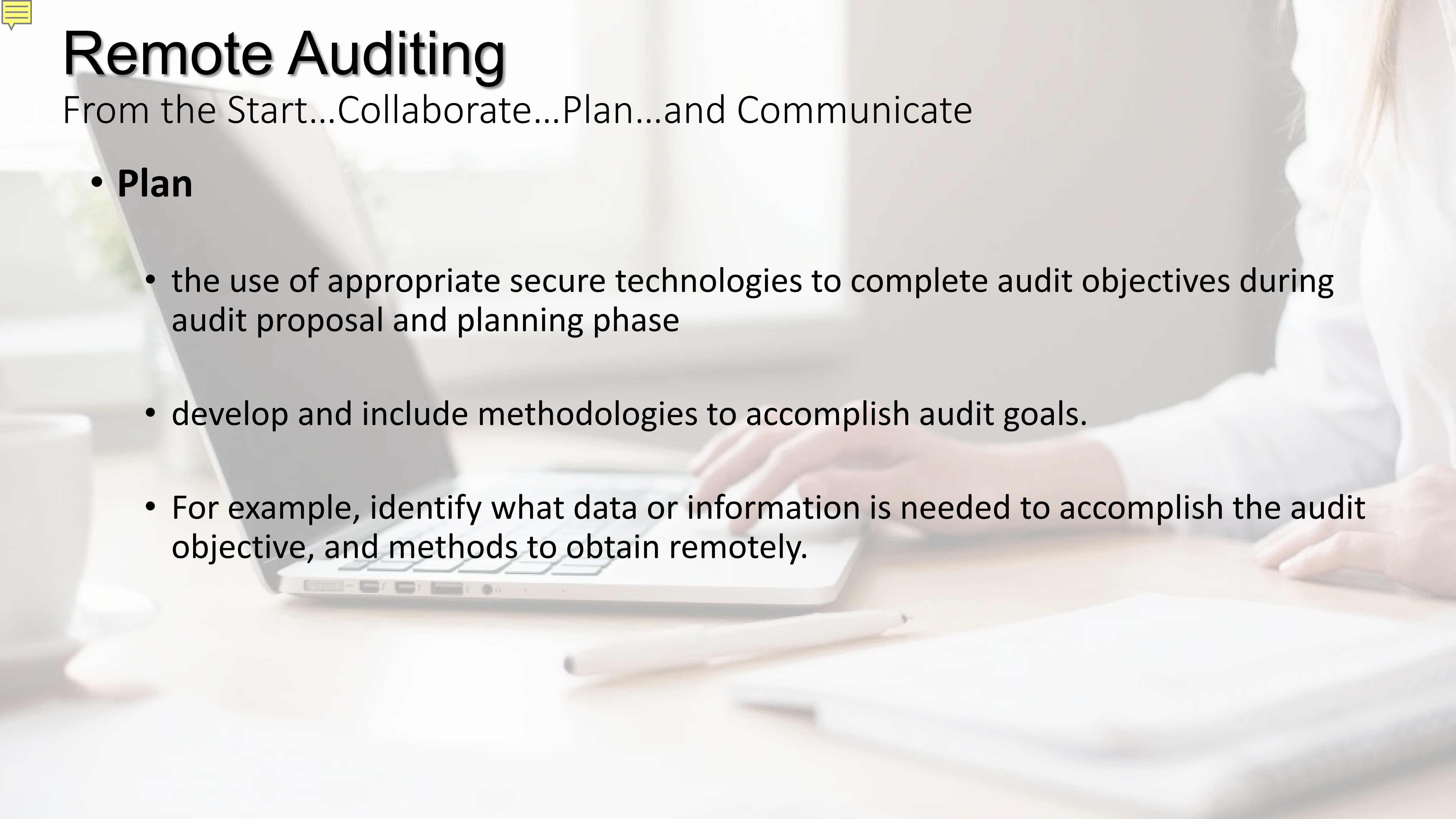
Remote Auditing

From the Start…Collaborate…Plan…and Communicate

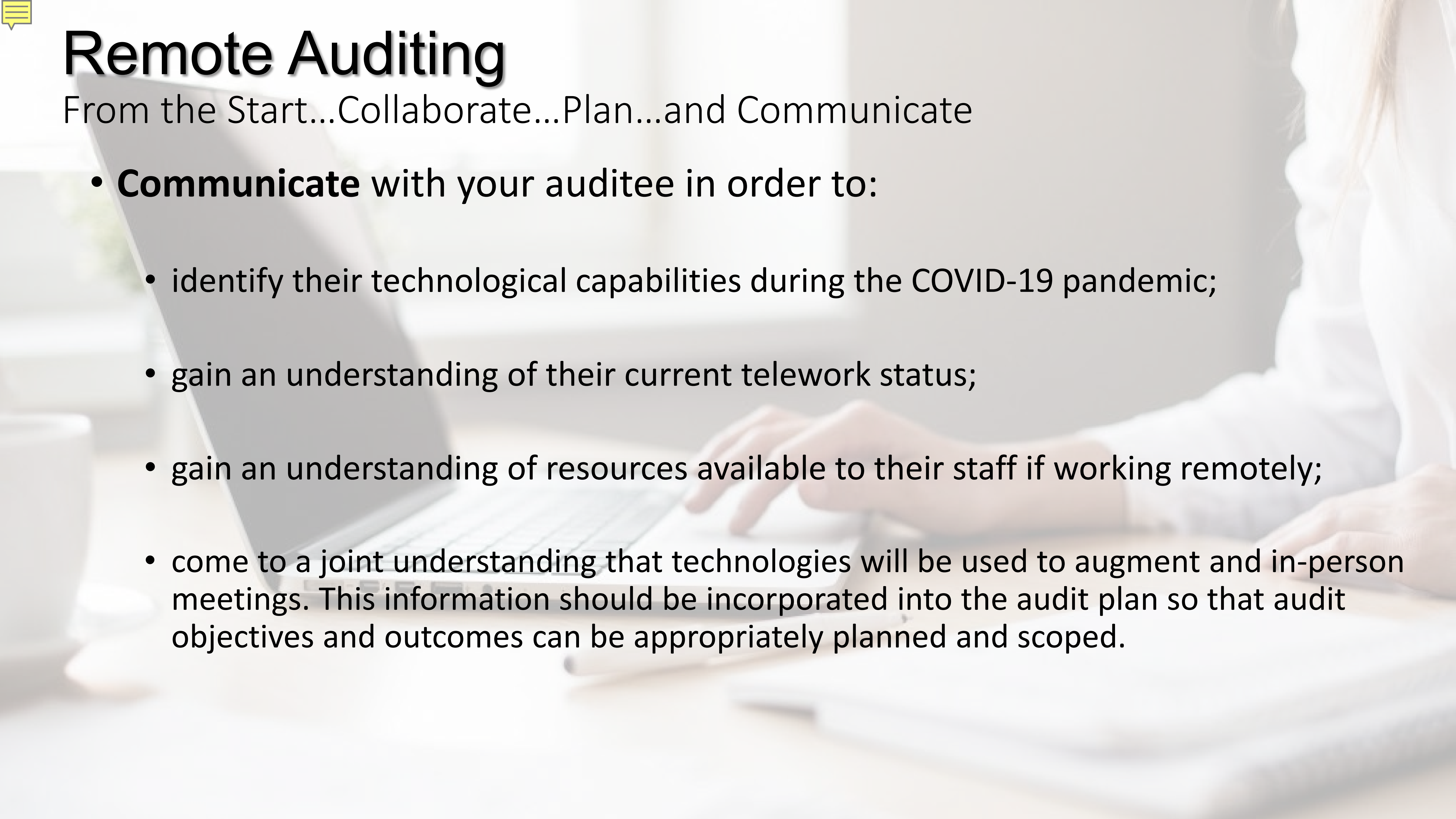
- **Collaborate**
- With your local information technology division, Helpdesk, or Chief Information Security Officer during the course of the audit in order to:
  - Identify in-house technological capabilities, (i.e., cloud sharing capabilities, Adobe Connect, MS Teams.) If possible:
  - Discuss audit topic, scope, and data or information needed to obtain during the course of the audit.
  - Discuss policy requirements and methods to keep information safe, such as confidentiality mechanisms like encryption and password protected files; and identity mechanisms such as digital signatures, and hashing.
- With your fellow audit staff and discuss technologies, methodologies, and processes they have used during their work and analysis.

Remote Auditing

From the Start…Collaborate…Plan…and Communicate



- **Plan**
  - the use of appropriate secure technologies to complete audit objectives during audit proposal and planning phase
  - develop and include methodologies to accomplish audit goals.
  - For example, identify what data or information is needed to accomplish the audit objective, and methods to obtain remotely.



Remote Auditing

From the Start…Collaborate…Plan…and Communicate

- **Communicate** with your auditee in order to:
  - identify their technological capabilities during the COVID-19 pandemic;
  - gain an understanding of their current telework status;
  - gain an understanding of resources available to their staff if working remotely;
  - come to a joint understanding that technologies will be used to augment and in-person meetings. This information should be incorporated into the audit plan so that audit objectives and outcomes can be appropriately planned and scoped.

Intergovernmental Audit Forum

23rd Biennial Forum of Government Auditors

Nicholas Marinos

GAO, Director, Information Technology and Cybersecurity