Guidehouse®

GOVERNMENT EXECUTIVE INTERVIEW

Cybersecurity, Quantum computing, and the recent restructuring of government

with Nancy Sieger, Partner, and Cindi Bassford, Partner

In a GovExec-moderated interview, Guidehouse's Nancy Sieger and Cindi Bassford surface several key themes, all pointing to a central issue: Quantum computing and the recent restructuring of government are the biggest risks to cybersecurity.

Q: As we begin the new year, what should be the top cybersecurity priorities for agencies?

CINDI BASSFORD: We've been predicting the end of traditional GRC for a while, but the way we now harvest data, operate with fewer resources, and rethink AI means we must use GRC tools very differently. We need to apply an engineering lens—automating evidence collection, enabling real-time decision-making, and moving away from treating GRC platforms as static documentation repositories.

We also need to get serious about post-quantum security. None of us know when quantum computers will be able to break modern encryption, but early estimates suggest it will cost millions to refresh networks when that moment arrives. If agencies understand their posture now, prioritize network refresh cycles, and put the right governance in place, they can substantially reduce the cost—and in some cases absorb it into normal O&M.

NANCY SIEGER: Quantum is absolutely at the top of my list. I believe the data has already been breached—quantum will eventually decrypt it. Foundations matter now more than ever. Agencies must reinforce access controls, maintain system currency, and ensure encryption for data at rest. Without those fundamentals, rapid technological change becomes fragile and unsustainable.

Q: What's next on the evolving threat landscape, and what should organizations be paying closest attention to?

CINDI BASSFORD: Identity and Access Management is overdue for a refresh. Zero Trust thrust IAM into the spotlight, transforming it from a security tool intoa business system. Agencies need a clear understanding of how AI and LLM tools are distributed throughout their environment and ensure that non-human identities—service accounts, automations, agents—are monitored and refreshed regularly. We must embrace AI quickly. Ouradversaries already are, and given the burnout across the cybersecurity workforce, AI is how we keep pace on both offense and defense.

NANCY SIEGER: I agree. Quantum remains a major concern, but so does strengthening foundational cyber hygiene. If those basics aren't solid, the speed of change will outpace our ability to secure it.

Q: With the rapid expansion of AI, what should agencies consider as they balance innovation with cybersecurity risk?

NANCY SIEGER: Government underwent major staff reductions in 2025. Systems are more brittle, and agencies have fewer people to maintain them. They must adopt what I call "resilient innovation"—continuing to innovate while adapting to staffing loss and the speed of technological change. Efficiencies without resilience will not last.

CINDI BASSFORD: Resilient innovation applies to people, processes, and technology. This isn't just a modernization cycle—it requires a whole-enterprise approach.

Q: How can agencies address the skills gap and upskill their workforce?

NANCY SIEGER: First, agencies must speed up the clearance process so outside experts can help more quickly and leave teams with the skills to sustain progress. They also need to reduce burnout and learn how to innovate so they can "do less with less" by letting AI handle routine work. Reinforcing the cybersecurity fundamentals will help them move faster into the future.

Q: What can government and industry do to strengthen cybersecurity collaboration?

CINDI BASSFORD: Recent attacks show we are only as strong as our weakest link. Government and industry must collaborate deeply—sharing information, shortening time to market, and learning from each other. FedRAMP 20X is a great example of productive collaboration. CISA's protections also help by allowing private companies to share information without fear of penalty, which strengthens the entire ecosystem.

NANCY SIEGER: As Guidehouse professionals, Cindi and I bring decades of hands-on cybersecurity delivery experience. We don't just talk about cybersecurity—we've built and run programs. My philosophy, as a former federal CIO, has always been: cybersecurity is everyone's responsibility.

Thank you for joining today's conversation. Don't forget to subscribe to GovTech Plus on YouTube for more discussions like this.

About Guidehouse

Guidehouse is a global AI-led professional services firm delivering advisory, technology, and managed services to the commercial and government sectors. With an integrated business technology approach, Guidehouse drives efficiency and resilience in the healthcare, financial services, energy, infrastructure, and national security markets. guidehouse.com/defense

Contacts:

Nancy Sieger
Partner
nsieger@guidehouse.com

Cindi Bassford
Partner, Cyber Leader
cbassford@guidehouse.com