

PRESS RELEASE

# Wiley Expands Cyber Practice with Erin Joe, Former Senior Leader from FBI, Mandiant, and Google Cloud

October 20, 2025

*Washington, DC* – Wiley is pleased to announce that Erin Joe has joined the firm as special counsel in its nationally recognized Privacy, Cyber & Data Governance Practice. Drawing on senior leadership roles at the Federal Bureau of Investigation (FBI) and in the private sector, Erin is a trusted advisor who has guided government and industry through some of the most pressing cyber and national security challenges of the past 20 years.

Most recently, Erin held senior leadership positions in Google Cloud's Office of the Chief Information Security Officer and at Mandiant, where she served as a strategic advisor to Fortune 100 companies and government entities on business resilience, regulatory readiness, and responses to emerging threats. She has counseled organizations on issues spanning national security, critical infrastructure, and the responsible adoption of new technologies, including cloud and artificial intelligence (AI), helping them strengthen defenses and meet evolving legal and compliance obligations.

"Erin adds to the deep FBI experience on our team, giving clients access to technical and operational support in cyber risk management as well as insight into national and international government responses to complex cyber threats," said Megan L. Brown, co-chair of Wiley's Privacy, Cyber & Data Governance Practice. "Her experience bridging government service and private-sector leadership strengthens our ability to guide clients through the legal, policy, and operational challenges of today's rapidly evolving threat environment."

## Related Professionals

Megan L. Brown  
Partner  
202.719.7579  
mbrown@wiley.law  
Erin M. Joe  
Special Counsel  
202.719.3140  
ejoe@wiley.law

## Practice Areas

Privacy, Cyber & Data Governance

Earlier in her career, Erin spent more than a decade at the FBI as a Legal Advisor and Acting Chief Division Counsel, where she counseled leadership on sensitive legal and policy matters, managed congressional and Inspector General inquiries, and shaped interagency policy on cyber and national security issues. She also led the Bureau's engagement with cleared defense contractors and telecommunications companies, coordinating multi-agency responses to nation-state intrusions and advising on legal, regulatory, and compliance considerations arising from complex cyber incidents.

At Wiley, Erin will advise clients on cybersecurity readiness, incident response, government investigations, congressional and regulatory inquiries, and M&A-related cyber due diligence. She will also counsel clients on governance, compliance, and crisis management strategies, expanding the breadth of the firm's capabilities to help organizations manage risk as they adopt new technologies.

"Wiley's focus on regulatory law, data privacy, government contracts, and technology is a perfect fit with my background," said Erin. "Businesses face constant pressure from cyber threats, and they need advisors who understand both the legal framework and the practical realities of incident response and government oversight. I've seen firsthand how unpreparedness can compound the legal, operational, and reputational impact of an attack, and I am excited to help clients anticipate risk, strengthen their resilience, and navigate these challenges with confidence."

Wiley's Privacy, Cyber & Data Governance Practice assists clients with a full spectrum of privacy, cybersecurity, and data governance issues, from compliance to transactional diligence to investigations, enforcement, and litigation. For more than 15 years, Wiley's multidisciplinary team has provided clients with a wide range and depth of service in privacy and cyber matters across sectors, including AI, tech, telecom, health care, government contracting, and financial services. Our practice spans federal, state, and international levels, featuring IAPP-certified attorneys and numerous former government officials, and we routinely advocate for sensible privacy and cyber approaches before government agencies.