

## Erin M. Joe

Special Counsel

 202.719.3140  
 [ejoe@wiley.law](mailto:ejoe@wiley.law)

Erin counsels clients on cybersecurity risk mitigation, incident readiness and response, crisis communications and management, evolving technologies, government investigations, congressional and regulatory inquiries, and M&A-related cyber due diligence. Drawing on over two decades of leadership, she advises clients on governance, compliance, and security strategies that address the legal, operational, and reputational dimensions of cyber risk. She frequently engages with senior executives across the public and private sectors to align legal, operational, and security priorities.

Erin previously held multiple leader roles at Mandiant, Google Cloud, and the Federal Bureau of Investigation (FBI), bringing front-line experience to address Wiley's client needs. Her government roles included serving as Director of the interagency Cyber Threat Intelligence Integration Center at the Office of the Director of National Intelligence and Deputy Assistant Director of the Cyber Division, where her work significantly accelerated federal cyber threat responses and shaped national-level crisis response and readiness. She led national and international cyber operations, developed the FBI's first comprehensive cross-program strategy to counter hostile cyber activity by nation-states, and orchestrated global responses to high-profile cyber incidents affecting critical infrastructure and Fortune 500 companies. For over 20 years, Erin has collaborated with private-sector companies, including defense contractors, building best practices to enhance their security and resilience. She has informed and advised the National Security Council (NSC), the U.S. Intelligence Community (IC), the White House, and Congress. Erin has also chaired interagency boards guiding U.S. government cyber strategy, served on private industry advisory boards for risk and cyber organizations, and shared insights as a thought leader and speaker.



## Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement  
Privacy, Cyber & Data Governance  
Telecom, Media & Technology

## Credentials

**Education**  
J.D., The Ohio State University Moritz College of Law  
B.A., University of Illinois  
**Bar and Court Memberships**  
Texas Bar

at over 100 industry events and engagements.

## Representative Matters

---

- Advises on complex national security, cybersecurity, technology, data, and privacy issues.
- Counsels and provides strategic guidance on security, resilience, and responsiveness to physical and cyber threats.
- Provides guidance to address cyber risk, reduce data and liability exposure, meet legal and regulatory requirements, and establish security programs that meet business needs.
- Advises clients on government investigations and actions.
- Provides crisis management advice and liaison services with responders and government before, during, and after cyberattacks.
- Oversees incident response investigations and cyber related assessments (privileged and nonprivileged)
- Federal government national security and cyber legal and policy experience at the FBI:
  - Oversaw threat intelligence integration and threat response preparation for 2020 elections and U.S. response to COVID-19.
  - Created frameworks that reduced U.S. government cyber threat response decision-making time from two weeks to less than 48 hours.
  - Developed national-level cyber crisis response plans with inputs from hundreds of private- and public-sector partners; led IC along with defense, financial, and energy sectors in creating cyber mitigation and prevention strategies to counter threats.
  - Developed the FBI's first comprehensive strategy to combat hostile cyber activity initiated by nation-states.
  - Orchestrated U.S. government teams and foreign ally responses against sophisticated attacks against large corporations, public figures, financial firms, hospitals, first responders, and other high-value targets.
  - Advised private-sector Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), Chief AI Officers, General Counsels, and law firms on novel legal issues and led collaboration enabling business decisions, risk assessments, and threat mitigation.

## Professional Experience

---

- Google Cloud and Mandiant, a Google Cloud company
  - Google Cloud Office of the CISO (2022-2025)

- Mandiant Senior Vice President (2021-2025)
- Senior Executive Advisor, Cybersecurity/Readiness/Digital Transformation (2021-2025)
- Federal Bureau of Investigation (FBI)
  - Senior Executive Service (SES) – Office of Private Sector (2020-2021)
  - SES – Director of Cyber Threat Intelligence Integration Center (2019-2020)
  - SES – Deputy Assistant Director and Section Chief of Cyber Division, Cyber Operations (2016-2020)
  - SES – Acting Special Agent in Charge – New Haven Division (Summer 2018)
  - SES – Section Chief, FBI Director’s Office of Partner Engagement (2015-2016)
  - Assistant Special Agent in Charge – Los Angeles Division (2013-2015)
  - Acting Assistant Special Agent in Charge/Supervisory Special Agent – Salt Lake City Division (2008-2013)
  - Supervisory Special Agent – Counterterrorism Division (2007-2008)
  - Supervisory Special Agent – Directorate of Intelligence (2005-2007)
  - Acting Chief Division Counsel/Special Agent – Oklahoma City Division (1996-2005)
- State of Texas: Workforce Commission
  - Administrative Law Judge/Hearing Officer (1993-1996)