Thank you for attending the FBI Cyber Division's engagement with attorneys from the Nation's leading cyber law firms on April 6, 2022 and April 11, 2022. The FBI Cyber Division Executive Team captured a tremendous amount of information from the collective group of attendees and have already started incorporating your reflections into strategic discussion here at FBI-Headquarters.

Receiving direct and honest feedback from leaders like you is extremely valuable to the FBI Cyber Program as we strive to build enduring and purposeful relationships with influential cyber law firms and their clients. Now that several days have passed to allow for reflection, I'm respectfully requesting your consideration and response to several questions designed to ensure FBI-Headquarters and our Field Offices remain collectively armed with information critical to performance improvement. Please know your *anonymous* (* or "confidential" as most appropriate) responses (*i.e. – we'd need a search warrant to identify each of you!*) will be read in-full and considered by FBI Cyber senior executives/senior leaders in our committed pursuit of ensuring the Nation's safety and security in a digitally connected world.

1. Considering the engagement on April 6th, what from this forum was ***most*** valuable to your firm's and/or clients' efforts in the cyber ecosystem as it pertains to potential relationships with the FBI?

2. Considering the engagement on April 6th, what should be included in future engagements (*i.e. classified threat/case briefings, etc.)* to add the most value to your firm and/or clients?

3. What recommendations do you have for ***FBI senior executives*** (*i.e. FBI Headquarters executive leader, FBI Field Office executive leaders, etc.)* to optimize federal law enforcement engagement, response, and investigative efforts with law firms specializing in cyber legal counsel and their clients?

4. What recommendations do you have for ***FBI field personnel*** *(i.e. Special Agents, Forensic/Response Teams, etc.)* to optimize federal law enforcement engagement, response, and investigative efforts with law firms specializing in cyber legal counsel and their clients?

5. When the FBI is conducting a victim notification (*i.e. USG intelligence indicates an adversary may have access to a company's system, etc.*), what looks like best-in-class service to your firm? To your clients? How should these notifications be made?

6. After a company has suffered a computer intrusion and during the FBI's response and investigative efforts (as part of a larger U.S. Government team), what looks like best-in-class service to your firm? To your clients?

7. During FBI response and investigative efforts (as part of a larger U.S. Government team), what should the FBI reasonably expect from your firm to ensure they can deliver best-in-class service? From your clients?

8. What else do you believe the FBI Cyber Program should account for as we continuously work to optimize our relationship with cyber law firms and their clients?

9. Are you open to further direct engagement with the FBI Cyber Division to help ensure we continue to improve our program?