

EBSA Privacy and Cybersecurity Guidance

Article By:

Andrew C. Liazos

Todd S. McClelland

Andrew C. Liazos, partner at McDermott Will & Emery, recently moderated an American Bar Association panel on the new cybersecurity guidance for retirement plan sponsors issued by the Department of Labor (DOL). The panel slides included 10 takeaways for the new DOL guidance.

[Access the slides.](#)

As a background, the DOL's new guidance formalized its long-held view that retirement plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks. More specifically, the DOL expects retirement plan fiduciaries to select and monitor the cybersecurity practices of their service providers.

The DOL guidance is in three parts.

- The first part provides plan fiduciaries with a framework for reviewing a vendor's cybersecurity practices.
- The second part provides a robust list of cybersecurity "best practices" for record keepers and other vendors responsible for plan-related IT systems and data. For example, the DOL recommends that all retirement plan vendors with critical participant data conduct a reliable annual third-party audit of their security controls.
- The third part provides security tips for participants and beneficiaries who manage their retirement accounts online.

Source URL: <https://natlawreview.com/article/ebsa-privacy-and-cybersecurity-guidance>