DOL Updates Cybersecurity Guidance

In its continuing effort to protect U.S. workers' retirement and health benefits, the U.S. Department of Labor updated current cybersecurity guidance confirming that it applies to all types of plans governed by the Employee Retirement Income Security Act, including health and welfare plans, and all employee retirement benefit plans.

The new Compliance Assistance Release issued by the department's Employee Benefits Security Administration provides best practices in cybersecurity for plan sponsors, plan fiduciaries, recordkeepers and plan participants. The release updates EBSA's 2021 guidance and includes the following:

- Tips for Hiring a Service Provider: Helps plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities, as ERISA requires.
- Cybersecurity Program Best Practices: Assists plan fiduciaries and recordkeepers in mitigating risks.
- Online Security Tips: Offers plan participants who check their online retirement accounts with rules for reducing the risk of fraud and loss.

As of June 2024, EBSA estimates ERISA covers 2.8 million health plans, 619,000 other welfare benefit plans and 765,000 private pension plans in America. These plans include 153 million workers, retirees and dependents who participate in private sector pension and welfare plans with $14 trillion in estimated assets. Without sufficient protections, digital participant and assets information may be vulnerable to the internal and external risks of computer-related crimes and losses. Federal regulations require plan fiduciaries to take appropriate precautions to mitigate these risks.

The Employee Benefits Security Administration believes cybersecurity is a great concern for all employee benefit plans and continues to investigate potential ERISA violations related to the issue.

The guidance complements EBSA’s regulations on electronic records and disclosures to plan participants and beneficiaries. These include provisions on ensuring that electronic recordkeeping systems have reasonable controls, adequate records management practices are in place and that electronic disclosure systems include measures calculated to protect Personally Identifiable Information.