DOL issues cybersecurity guidance for retirement plans

By Brian J. Kearney, Margaret Berger and Katharine Marshall
April 26, 2021

In this article

In response to a recommendation by the Government Accountability Office (GAO), the Department of Labor (DOL) has issued three pieces of informal cybersecurity guidance for retirement plans. One document suggests how plan fiduciaries can prudently select service providers with strong cybersecurity practices and monitor providers' activities. The second document recommends cybersecurity best practices for recordkeepers and other service providers responsible for plan-related information technology (IT) systems and personally identifiable information (PII). The third document gives tips for participants to keep their online accounts secure. Plan fiduciaries should review their current practices and existing service contracts for consistency with the new guidance. Although the guidance is directed toward retirement plans, its applicability to other types of ERISA plans is unclear.

GAO request for guidance

In a recent report to leaders of House and Senate committees that oversee retirement plans, GAO recommended that DOL formally state whether retirement plan fiduciaries are legally responsible for mitigating cybersecurity risks. In response, DOL officials told GAO that they believe ERISA requires fiduciaries to take appropriate precautions to reduce cybersecurity risks to retirement plan assets and PII. However, while the new publications make clear that cybersecurity is a fiduciary concern, DOL has yet to say so in a regulation or other formal guidance.

GAO also urged DOL to issue guidance identifying minimum expectations for reducing cybersecurity risk, including specific steps plans should take to protect participant accounts and PII. DOL agreed that increasing awareness of fiduciary responsibilities with respect to cybersecurity would be helpful and said it was drafting compliance material toward that end. The new guidance makes specific recommendations for both plans and service providers. While the guidance is subregulatory, it makes clear that DOL expects plan fiduciaries, recordkeepers and other service providers to follow its cybersecurity recommendations and may even look for compliance during audits.

DOL's three-part guidance

The new guidance package has separate documents for plan sponsors and fiduciaries, service providers, and participants.

Tips for fiduciaries contracting with service providers. In a news release announcing the guidance, DOL says ERISA requires plan fiduciaries to prudently select service providers with strong cybersecurity practices and monitor providers' activities. To help fiduciaries fulfill these duties, DOL has published a tip sheet urging plan sponsors and fiduciaries to ask for a host of information about a service provider's cybersecurity program, such as details about the provider's cybersecurity practices, its track record and any past breaches. Another relevant question is whether the provider has insurance policies that would cover cybersecurity and identity theft breaches.

DOL also recommends negotiating for certain contract provisions to enhance cybersecurity protection. Examples include specific terms detailing the service provider's obligations to protect PII, requiring the provider to obtain third-party audits of its practices and ensuring the plan's right to review the audit results. Fiduciaries should also consider requiring the service provider to obtain insurance coverage and avoid contract provisions limiting the provider's responsibility for IT security breaches.

Best practices for cybersecurity programs. The new guidance identifies 12 cybersecurity best practices for recordkeepers and other service providers responsible for plan-related IT systems and data. The best practices are practical in nature, addressing topics such as ensuring the safety of information stored in a cloud, encrypting sensitive data (both in storage and transit), and conducting periodic cybersecurity awareness training for employees. The best practices also include some of the items DOL recommends plan fiduciaries request when hiring service providers, such as a formal written cybersecurity program and annual third-party audits. The guidance says plan fiduciaries should look for a service provider's adherence to these practices when making prudent hiring decisions.

Tips for participants on keeping accounts secure. The tips for plan participants focus on a range of issues for online security, including regularly monitoring online accounts, using strong passwords and multifactor authentication, keeping contact information current, exercising caution with free wireless internet connections, and avoiding viruses and phishing attacks. The document includes links to the FBI and Department of Homeland Security websites for reporting cybersecurity incidents.

Application to other ERISA plans?

The GAO report discussed cybersecurity for retirement plans, and DOL's news release suggests that the new publications likewise focus on those plans. However, the extent to which the guidance applies to other ERISA plans is unclear. The tips on hiring and monitoring service providers are addressed specifically to retirement plan fiduciaries, while the best practices document appears to discuss ERISA plan service providers in general. However, the guiding principles of both documents seem relevant to all ERISA plans, as all fiduciaries have an obligation to prudently select and monitor service providers.

The Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act and implementing regulations already prescribe rules for health plans to secure electronic protected health information (PHI). Other ERISA-covered plans, such as disability, life and some on-site clinics, aren't subject to the privacy and security rules for health plans but still face similar cybersecurity risks. If the guidance is meant to explain how ERISA fiduciaries can satisfy their duty to prudently monitor and select service providers, sponsors of these other plans might find the DOL guidance useful. Employers may want to discuss with counsel the implications of the guidance for all ERISA plans.

Related resources

Non-Mercer resources

- Tips for hiring a service provider with strong cybersecurity practices (DOL, April 14, 2021)
- Cybersecurity program best practices (DOL, April 14, 2021)
- Online security tips (DOL, April 14, 2021)
- News release (DOL, April 14, 2021)
- Defined contribution plans: Federal guidance could help mitigate cybersecurity risks in 401(k) and other retirement plans (GAO, March 15, 2021)

Mercer Law & Policy resource

- DOL urged to give retirement plans cybersecurity guidance (April 7, 2021)

Note: Mercer is not engaged in the practice of law, accounting or medicine. Any commentary in this article does not constitute and is not a substitute for legal, tax or medical advice. Readers of this article should consult a legal, tax or medical expert for advice on those matters.