

# DOL Puts Plan Sponsors and Other Fiduciaries on Notice: ERISA Requires Appropriate Precautions to Mitigate Cybersecurity Threats

---

*April 20, 2021*

There just may be a new cybersecurity regulator in town.

In an effort it describes as “an important step” toward safeguarding more than \$9.3 trillion in retirement assets, the U.S. Department of Labor (DOL) published its first cybersecurity guidance last week ([Cybersecurity Guidance](#)). The Cybersecurity Guidance is directed at plan sponsors and fiduciaries regulated by the [Employee Retirement Income Security Act](#) of 1974 (ERISA) as well as plan participants and beneficiaries. Significantly, the Cybersecurity Guidance formally states the DOL’s position that cybersecurity is a matter of fiduciary responsibility under ERISA, stating that ERISA requires plan fiduciaries to take appropriate precautions to mitigate cybersecurity risks.

The DOL also highlighted that the Cybersecurity Guidance was designed to “complement” existing Employee Benefits Security Administration (EBSA) regulations on electronic records and disclosures to plan participants and beneficiaries. This development indicates that sponsors and fiduciaries may soon be subject to focused scrutiny over their cybersecurity practices in DOL investigations and adds to the multiple existing sources of cybersecurity legal risk in the wake of data breaches or insufficient cybersecurity controls. Critically, the Cybersecurity Guidance does not weigh in on the issue of whether ERISA would preempt cybersecurity regulations or laws at the state level — often a driving source of cybersecurity legal risk.

The Cybersecurity Guidance is set forth in three parts:

- [Tips for Hiring a Service Provider](#), directed toward plan sponsors and fiduciaries
- [Cybersecurity Program Best Practices](#) (Best Practices), directed at recordkeepers and other service providers responsible for plan-related IT systems and data as well as plan fiduciaries evaluating service providers’ cybersecurity programs
- [Online Security Tips](#) for plan participants and beneficiaries.

## Considerations for Plan Sponsors and Other Fiduciaries

Although the Cybersecurity Guidance does not provide a minimum standard or safe harbor approach for mitigating cybersecurity risks, plan sponsors and other fiduciaries would be wise to assess the strength of their current cybersecurity practices and risk mitigation efforts against the best practices and tips set forth in Cybersecurity Guidance, which indicates that such plan sponsors and fiduciaries should do the following:

1. Select and monitor service providers with an eye toward cybersecurity. DOL guidance provides a series of questions that should serve as a starting point for this review and includes topics such as the service provider's information security standards, track record, cybersecurity insurance coverage, and cybersecurity validation techniques. A formal vendor selection program that maintains records of vendors' responses to the questions would further strengthen the program's maturity and the plan sponsor's ability to demonstrate compliance with the Cybersecurity Guidance. Plan sponsors and fiduciaries should carefully review the full list of Tips for Hiring a Service Provider.
2. Conduct periodic reviews of the cybersecurity programs of recordkeepers and other service providers responsible for plan-related IT systems and data and request that service providers demonstrate the manner in which their cybersecurity program reflects Best Practices.
3. Review the terms of agreements with service providers to ensure they require ongoing compliance by the service providers with cybersecurity and information security standards and contain best practice provisions such as requiring prompt notification of cybersecurity breaches. Some of the recommended contractual provisions are robust, including a recommendation that "[t]he contract should require the service provider to annually obtain a third-party audit to determine compliance with information security policies and procedures." The Cybersecurity Guidance also recommends provisions to "prevent the use or disclosure of confidential information without written permission." At a minimum, plan sponsors should review their existing contracts and make efforts to address the list of contract provisions DOL suggests in its list of Tips for Hiring a Service Provider.
4. Educate participants and beneficiaries who manage their retirement accounts online about online security. To the extent recordkeepers or other service providers already offer participants and beneficiaries training of this nature, they should review existing materials to confirm that they reflect all of the Online Security Tips.

### **Obligations of Service Providers Responsible for Plan-Related IT Systems and Data**

Service providers who must comply with the Best Practices should implement the following: a documented cybersecurity program; annual risk assessments; clearly defined and assigned roles and responsibility for cybersecurity risk management; strong access controls; cybersecurity awareness training; encryption for sensitive data at rest and in transit; secure system development lifecycle program; third-party reviews and audits; business continuity planning; and cybersecurity incident response. The Best Practices highlight 18 areas of cybersecurity controls appropriate for policies approved by senior leadership, which emphasize the "documented" nature of the recommended cybersecurity program. Critically, while the Best Practices do not specifically require multifactor authentication (MFA) as part of the "strong access controls," the Online Security Tips extol participants to "use multi-factor authentication" to "reduce the risk of fraud and loss," which creates clear pressure on service providers to enable MFA features in online accounts.

These recommendations are largely in line with certain other existing standards requiring a formal cybersecurity program, including the National Association of Insurance Commissioners Insurance Data Security Model Law, the New York Department of Financial Services Cybersecurity Regulations, and the Massachusetts Office of Consumer Affairs and Business Regulation Cybersecurity Regulations. The Cybersecurity Guidance also is in line with well-known industry standards, specifically referencing the Identify, Protect, Detect, Recover, Disclose and Restore functions put forth by the National Institute of Standards and Technology Cybersecurity Framework.

## CONTACTS

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work, or

<b>Colleen Theresa Brown</b> , Partner	+1 202 736 8465, <a href="mailto:ctbrown@sidley.com">ctbrown@sidley.com</a>
<b>Mary C. Niehaus</b> , Partner	+1 312 853 6090, <a href="mailto:mniehaus@sidley.com">mniehaus@sidley.com</a>
<b>Teresa A. Napoli</b> , Partner	+1 312 853 0823, <a href="mailto:tnapoli@sidley.com">tnapoli@sidley.com</a>

---

Attorney Advertising—Sidley Austin LLP is a global law firm. Our addresses and contact information can be found at [www.sidley.com/en/locations/offices](http://www.sidley.com/en/locations/offices).

Sidley provides this information as a service to clients and other friends for educational purposes only. It should not be construed or relied on as legal advice or to create a lawyer-client relationship. Readers should not act upon this information without seeking advice from professional advisers. Sidley and Sidley Austin refer to Sidley Austin LLP and affiliated partnerships as explained at [www.sidley.com/disclaimer](http://www.sidley.com/disclaimer).

© Sidley Austin LLP