Published on *The National Law Review* https://natlawreview.com

U.S. Department of Labor Steps into the Cybersecurity Discussion

Article By:

Robert M Projansky

Steven D Weinstein

Randall Bunnell

Formally wading into the cybersecurity discussion for the first time, on April 14, 2021, the U.S. Department of Labor (DOL) posted on its website a suite of new guidance, including Tips for Hiring a Service Provider with Strong Cybersecurity Practices, Cybersecurity Program Best Practices, and Online Security Tips for Participants and Beneficiaries.

By way of background, cybersecurity has over the last decade become an area of critical importance to sponsors and administrators of employee benefit plans as well as plan participants. Put simply, this is because plans (which the DOL estimates hold $9.3 trillion in assets) are a prime target of cyberthieves, given that they typically hold significant amounts of sensitive participant data, often permit electronic access to funds (think 401(k) distributions) and rely on outside service providers, who provide additional access points for breach. This risk was only exacerbated by the COVID-19 shutdowns, where benefits personnel and their service providers quickly had to transition to working remotely and begin relying on electronic access more than ever before.

In the face of these cybersecurity challenges, many plan sponsors and administrators have considered ways to mitigate risk, both internally (*e.g.*, through education of their benefits personnel and participants) and externally (principally through management of their service provider relationships).

In recent years, it has been suggested (including by the Government Accountability Office in a February 2021 report) that the DOL should provide its perspective on fiduciary responsibilities with respect to cybersecurity. Until now, the DOL has been largely silent on these matters, but has now stepped into the discussion with the following three pieces of guidance aimed at three different audiences.

Cybersecurity Program Best Practices: This document contains a list of 12 best practices for use by recordkeepers and other plan service providers responsible for information technology and data. This guidance provides fairly extensive detail for each of the 12 items, which range from a description

of what the DOL expects to see in a formal, documented cybersecurity program to stressing the importance of annual internal risk assessments along with external audits of security controls. The document also details the actions that should be taken in the event a cybersecurity breach or incident occurs. While this document is principally aimed at controls for service providers, it would still be relevant for plans that maintain information technology systems in-house. Even for plans that do not maintain in-house systems, the DOL indicated that these best practices are for use by plan fiduciaries in their vendor hiring decisions. Notably, the DOL has a blanket statement in this document that "plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks."

Tips for Hiring a Service Provider with Strong Cybersecurity Practices: The DOL then turned its focus directly to plan fiduciaries, issuing a document that provides some succinct suggestions for steps that plan sponsors and administrators might take with respect to diligence of, and contracting with, plan service providers. For example, the DOL guidance suggests the following steps:

- Ask about the provider's cybersecurity program and compare it to industry standards. As noted above, the DOL's twelve Cybersecurity Program Best Practices can serve as useful guidance on the DOL's view of what constitutes a sound cybersecurity program.

- Seek providers that engage a third-party auditor to annually review and validate its cybersecurity program. The DOL further suggests that plan fiduciaries include a provision in the contract with the provider requiring that an annual third-party cybersecurity compliance audit be conducted.

- Evaluate the provider's track record in the industry by reviewing publicly available information about past security incidents and legal proceedings involving the provider.

- Ask about past security breaches and how the provider responded.

- Ask about the provider's insurance policies that would cover losses caused by cybersecurity and identity theft breaches and consider requiring the provider to maintain professional liability and errors and omissions liability insurance, cyber liability and privacy breach insurance, and/or fidelity bond/blanket crime coverage.

- Negotiate clear provisions in the contract regarding the provider's obligation to keep private information private and meet a strong standard of care to protect confidential information.

- The provider contract should require the provider's ongoing compliance with internal cybersecurity and information security standards as well as compliance with records retention and destruction, privacy and information security laws.

- Include in the provider contract how much time the provider has to provide notice to the fiduciary of a security breach and require that the provider investigate and reasonably address the cause of the breach. The DOL also states that plan fiduciaries should carefully review contract provisions that would limit the provider's responsibility for cybersecurity breaches.

Online Security Tips for Participants and Beneficiaries: Apparently recognizing that participants and beneficiaries represent a primary vulnerability from a cybersecurity perspective, the DOL provided these security tips for participants to consider in order to reduce the risk of fraud or cybertheft with

respect to their benefits. This list contains many predictable, but important, topics such as strong password use, phishing awareness, updating personal contact information and monitoring accounts. While the DOL did not specifically suggest this, plan sponsors and administrators may wish to consider disseminating this guidance (or their own version of the guidance) to participants to improve their cybersecurity awareness and help avoid future crises.

The View from Proskauer

Given the threat that cybercrime poses to plans in the post-COVID world, it is an excellent time for plan sponsors and administrators to analyze their own vulnerabilities and establish an action plan to mitigate the risk of loss associated with data security breaches. Vendor diligence and contracting is a critical – albeit not the sole – component of such an action plan. The DOL's guidance provides a helpful look into the DOL's perspective on this issue and should be considered as a useful data point in the broader analysis.

National Law Review, Volume XI, Number 105