DOL Issues Cybersecurity Guidelines and Begins Audits

Victoria E. Anderson

November 22, 2021

To address growing cybersecurity risks to plan participants and their retirement assets, the Department of Labor (DOL) issued a set of guidance for retirement plan sponsors and fiduciaries, their service providers, and plan participants aimed at mitigating cybersecurity risks. The DOL has also begun examining plans' cybersecurity programs. Its information requests, which are very detailed and encompassing, signal that the guidelines are not optional and that the DOL is serious about enforcing them. The below is a summary of the DOL's guidance and items it has signaled will be reviewed in a cybersecurity audit.

DOL Guidance The DOL released its guidance on April 14, 2021 in three pieces. The first piece, "Tips for Hiring a Service Provider," is aimed at assisting plan sponsors and fiduciaries in choosing service providers with robust cybersecurity practices. The initial guidance makes clear that the DOL considers the management of cybersecurity risk – including the scrutinizing of service providers' cybersecurity policies and practices – to be part of a fiduciary's duties. The tips include:

- Making sure that contracts with service providers require their ongoing compliance with cybersecurity and information security standards, and being wary of provisions that limit the service provider's responsibility for IT security breaches;
- Looking for contract provisions that give plan sponsors and fiduciaries the right to review the service provider's audit results demonstrating compliance with industry security standards;
- Examining the service provider's track record in the industry, including public information regarding information security incidents;
- Inquiring as to any past security breaches, how they came about, and how the service provider responded; and
- Finding out whether the service provider has any insurance policies that would cover losses caused by cybersecurity and identity theft breaches, whether internal or external.

The second piece of guidance, "Cybersecurity Program Best Practices," advises plan fiduciaries and record-keepers on their responsibilities to manage cybersecurity risks. These include:

- Conducting prudent annual risk assessments;
- Conducting periodic cybersecurity awareness training for employees;
- Having an effective business resiliency program addressing business continuity, disaster recovery, and incident response in the event of disruption due to a security incident; and

- Encrypting sensitive data, both stored and in transit.

Plan sponsors may also wish to engage information technology assistance to the extent it would help them meet these requirements.

The third piece of guidance, “Online Security Tips,” is directed at plan participants and beneficiaries who check or manage their retirement accounts online and includes such tips as:

- Using strong and unique passwords;
- Using multi-factor authentication;
- Recognizing phishing attacks; and
- Using antivirus software.

Note that although this third set of guidance is geared toward participants and beneficiaries, employers and plan sponsors would also be well-served to engage an administrator that tries to enhance cybersecurity awareness on the participants’ side (for example, by informing and/or reminding participants to take the above actions).

Audit Initiative The type of documentation that the DOL has requested as part of its recent audits is quite comprehensive, including basically all information and documentation that an organization has relating to its information security systems. A few examples of such requests include:

- All policies, procedures, or guidelines relating to:
    - Data governance, classification, and disposal
    - The implementation of access controls and identity management, including any use of multi-factor authentication
    - The processes for business continuity, disaster recovery, and incident response
    - The assessment of security risks
    - Data privacy
    - Management of vendors and third party service providers, including notification protocols for cybersecurity events and the use of data for any purpose other than the direct performance of their duties
    - Cybersecurity awareness training
    - Encryption to protect all sensitive information transmitted, stored, or in transit.
- All documents and communications relating to any past cybersecurity incidents.
- All documents and communications from service providers regarding policies and procedures for collecting, storing, archiving, deleting, anonymizing, warehousing, and sharing data.
- All documents and communications describing the permitted uses of data by the sponsor of the plan or by any service providers of the plan, including, but not limited to, all uses of data for the direct or indirect purpose of cross-selling or marketing products and services.

What this Means for Plan Sponsors and Fiduciaries In light of the DOL's apparent focus on protecting plan participants from cybersecurity threats, plan sponsors and fiduciaries should consider how much of the above documentation they can provide in the event of an audit. Where there are identified weaknesses in their cybersecurity programs, they should act to address them to bring them in line with the DOL guidance prior to being audited.

Furthermore, plan sponsors and fiduciaries should look into the cybersecurity practices of their service providers and, where necessary, implement the recommendations in the DOL guidance pertaining to their contracts with their service providers. For example, they should ensure that the contracts include provisions requiring the service provider to obtain annual third-party audits to determine compliance with information security policies and procedures, to provide notification within a specified timeframe in the event of any cyber incident or data breach, to cooperate to investigate and address the cause of the breach, and to obtain some form of cyber liability insurance coverage.

Employers might also consider reminding their employees of the importance of protecting their retirement plan accounts using the guidance in the DOL's "Online Security Tips."

If you have any questions about the DOL's cybersecurity guidance, would like assistance in implementing best practices, or need help in responding to an audit, please contact a member of our Employee Benefits Group.