Insights, News & Events

DOL CYBERSECURITY GUIDANCE: MANAGING RISKS TO EMPLOYER-SPONSORED RETIREMENT PLANS

Publication
Jun 1, 2021

The Government Accountability Office recently urged the U.S. Department of Labor to release guidance on cybersecurity matters in an effort to mitigate risks to 401(k) and other retirement plans. The GAO noted that there were trillions of dollars in employer-sponsored defined contribution retirement plans and that the DOL had not clarified whether plan fiduciaries have any responsibility regarding cybersecurity issues. On April 14, the DOL confirmed that employee benefit plan fiduciaries have an obligation to manage cybersecurity risks to their employer-sponsored plans.

In issuing this guidance, the DOL recognized that plan fiduciaries have a duty to mitigate cybersecurity risks. Without sufficient protections, the estimated 34 million defined benefit plan participants in private pension plans and 106 million defined contribution plan participants covering $9.3 trillion in assets may be at risk from cybersecurity threats. Accordingly, ERISA requires plan fiduciaries to take appropriate precautions to mitigate the risk. The DOL's cybersecurity guidance was released in three parts:

1. Tips for Hiring a Service Provider with Strong Cybersecurity Practices, which provides guidance to plan fiduciaries in the hiring of service providers;

Service Focus

Employee Benefits and Tax

Privacy and Cyber

2. Cybersecurity Program Best Practices, which provides best practices for recordkeepers and other service providers; and

3. Online Security Tips, which provides advice to plan participants and beneficiaries who check and manage their accounts online.

This guidance was published in the form of "tips" with some suggested "best practices" primarily for plan fiduciaries to consider, rather than establishing required steps or measures for plan fiduciaries to take. However, the Tips for Hiring a Service Provider and Cybersecurity Program Best Practices are sufficiently detailed that it would not be surprising if the DOL began to consider these steps as the minimum expectations for plan fiduciaries to comply with their obligations to manage cybersecurity risks.

It is worth noting that the GAO urged the DOL to release guidance relating to retirement plans and cybersecurity considerations in light of the trillions in assets held in such plans. The DOL's guidance is similarly geared to retirement plans, particularly the Tips for Hiring a Service Provider document, despite being directed at plan sponsors and fiduciaries regulated by the Employee Retirement Income Security Act (ERISA). While this guidance may not explicitly refer to employer-sponsored plans other than retirement plans governed by ERISA, plan fiduciaries should consider the tips and best practices for other plans, to the extent applicable. This is particularly true for other plans governed by ERISA, such as health and welfare plans, because the same fiduciary responsibilities applicable to retirement plans would apply to health and welfare plans as well.

Tips for Hiring a Service Provider

Sponsors of retirement plans are no strangers to hiring service providers to work with their retirement plans and, accordingly, are familiar with the requirement to ensure a prudent process for the selection and monitoring of such service providers. This guidance

now sweeps cybersecurity considerations into the topics of consideration when selecting service providers.

The DOL provides suggested questions to ask potential service providers in order to gauge that service provider's cybersecurity practices. This includes asking the service provider about their information security standards, audit policies and results, how it validates its practices, what levels of security standards it has met and implemented, and past security breaches. The responses should be considered against other potential service providers, industry standards, and the service providers track record.

Beyond just questions, the DOL guidance suggests careful attention to the service contract. Under this DOL guidance, the service contracts should, among other things:

- Require the service provider to obtain third-party audits on an annual basis;
- Identify how quickly a service provider must inform plan fiduciaries of breaches; and
- Specify the service provider's obligation to meet applicable federal, state, and local laws regarding privacy, confidentiality, or security or participant's personal information.

Cybersecurity Program Best Practices

The DOL has identified a 12-point best practice system for use by recordkeepers for plan-related IT systems and for use by plan fiduciaries in making prudent decisions regarding cybersecurity measures. In brief, the 12 points identified by the DOL are:

1. Have a formal, well-documented cybersecurity program. This includes a system to identify risks, protect assets, data and systems, detecting and responding to cybersecurity events, recovering from the event, disclosing (as appropriate), and restoring normal operations and services. This program

should be approved by senior leadership, reviewed internally at least annually, and should be reviewed by an independent third-party auditor to assess compliance and threats.

2. Create a prudent, annual risk assessment program. A manageable, effective risk assessment schedule should be established to identify and assess cybersecurity risks and to describe how the program will mitigate identified risks. This program should be updated to account for changes to information systems, service providers, or other changes to business operations.

3. Engage a third-party annual audit of the security controls. In addition to the internal measures adopted, an independent third-party auditor should assess the security controls on an annual basis. If the auditor's report identifies any weaknesses, the plan fiduciary should also document the correction of any identified weaknesses.

4. Clearly define and assign information security roles and responsibilities. Related to the first and second point, a prudent system to manage cybersecurity risks should clearly identify who has responsibility for each aspect of the program. The DOL specifically contemplates that a cybersecurity program must be managed at the senior executive level and then executed by qualified personnel. The Chief Information Security Officer (CISO) would generally be an appropriate individual to establish and maintain the program.

5. Ensure strong access control procedures. A strong procedure should be established to guarantee that users are who they say they are and that only approved users are able to access IT systems and data. This would require an appropriate system of authentication and authorization.

6. Assess third-party service provider use of cloud computing. The security programs and features of the cloud service provider should be assessed as

part of the decision to engage with such service provider. This would include requiring a risk assessment of the third-party service provider, periodically assessing the service provider, and ensuring that the guidelines of any safety program are satisfied. The Tips for Hiring a Service Provider, discussed above, would apply to cloud service providers.

7. Conduct annual cybersecurity awareness training. A strong procedure should address risk from each level, including the employee level. Accordingly, the DOL suggests conducting an annual cybersecurity awareness to educate everyone to recognize attacks, help prevent incidents, and guard against identify theft.

8. Implement a secure system development life cycle (SDLC) program. A secure SDLC program ensures that security assurance activities, such as code review, are an integral part of the system development process.

9. Implement a business resiliency program to address business continuity, disaster recovery, and incident response. Business resilience is the ability to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets, and data. The DOL proposes creating a business continuity plan, disaster recovery plan, and an incident response plan.

10. Encrypt sensitive data. A cybersecurity system should implement current, prudent standards for encryption data that is stored and for data that is transmitted.

11. Implement strong technical controls to implement best security practices. Technical security controls should be implemented that keep hardware, software, and firmware up to date, conduct routine data backup, and ensure routine patch management.

12. Be responsive to cybersecurity incidents or breaches. Ensure appropriate action is taken to protect the plan and plan participants in the event of a cybersecurity incident or breach. Such action may include informing law enforcement, notifying insurers, investigating the incident, and fixing the problem or weakness that caused the breach.

Online Security Tips

The final component of the DOL guidance focuses on steps and actions that plan participants and beneficiaries can take to mitigate potential cybersecurity risks on their end. These tips include regular monitoring of their accounts, the use of strong passwords with multi-factor authentication, updating personal contact information, and signing up for account activity notices. As part of this advice, the DOL also provides individuals with some general best practice considerations when accessing accounts or having an online presence generally, such as being aware of phishing attacks, the use of antivirus software, and the necessity to update and keep apps and software current.

Moving Forward with the DOL Guidance

Cybersecurity has been an increasing concern across the board as processes and platforms have increasingly moved to remote or electronic providers. Given this landscape of electronic services and the DOL's recent guidance, plan fiduciaries should review and analyze the processes currently in place to address cybersecurity risks.

Plan fiduciaries should also review their current service provider contracts and hiring processes, particularly for any contracts that are coming up for renewal or termination. The DOL's guidance will need to be weighed against current practices of plan sponsors and plan fiduciaries and, if there are any gaps, some additional steps may be required to ensure plan fiduciaries are able to fulfill all of their obligations when it comes to cybersecurity concerns.

For further information, contact your Fisher Phillips attorney, the author of this article, or any member of our Employee Benefits and Tax Practice Group. We will continue to monitor the latest developments and provide updates as appropriate, so make sure you subscribe to the Fisher Phillips Insight system by clicking here.