Department of Labor Intensifies Cyber Readiness Inquiries Among Retirement Plan Administrators

July 13, 2021

In light of recent reports of an increase in cybersecurity inquiries by the U.S. Department of Labor (the "DOL"), retirement plan administrators should accelerate their preparedness strategies for avoiding and addressing cybersecurity attacks against retirement plans. Media outlets are reporting that the DOL's Employee Benefits Security Administration has begun asking plan sponsors questions related to cybersecurity policies and procedures.

The increase in DOL inquiries, while unsurprising in light of the many recent headlines involving cyber and the trillions of dollars of assets located in retirement plans, are surprising in light of the short amount of time that has elapsed since the DOL first published a summary of best practices in this area. Retirement plan administrators should act to avoid being caught off guard by the possibility of DOL focus in this key area, which we expect to form part of any DOL inquiry for the foreseeable future. Importantly, many of the areas addressed by the summary involve fiduciary determinations (as opposed to non-fiduciary areas of plan design and administration), creating an added urgency to address cyber readiness for retirement plans.

As background, in April, the DOL issued a list of best cyber readiness practices for retirement plan administrators (as well as a separate list of best practices for plan participants). That guidance may be found here. The April guidance encourages plan administrators to:

- **Have a formal, well-documented cybersecurity program**. This program would consist of formal procedures to identify risks; protect assets, data and systems; detect and respond to cybersecurity events; recover from a breach; make any required disclosures; and restore normal operations and services. The documentation for this program should be reviewed at least annually and updated as appropriate.

- **Conduct prudent annual risk assessments**. Retirement plan administrators should establish an annual risk-assessment schedule. Changes in business operations, service providers and information systems should drive the timing and content of updates.

- **Have a reliable annual third-party audit of security controls**. An independent third-party auditor should identify risks and weaknesses for the plan fiduciary to address. Though not mentioned by the DOL, this expense (and other third-party expenses incurred in connection with cyber readiness) should generally be able to be charged to the plan if the plan document so permits.

- **Clearly define and assign information security roles and responsibilities**. A prudent system to manage cybersecurity risks should clearly identify who has responsibility for each aspect of the program. The DOL contemplates that a cybersecurity program must be managed at the senior executive level (i.e., by a Chief Information Security Officer or equivalent senior executive) and then executed by qualified personnel who are subject to background checks.

- **Have strong access-control procedures**. These procedures entail an appropriate system of authentication and authorization to guarantee that users are who they say they are and that only approved users are able to access IT systems and data. Multifactor authentication should be implemented wherever possible, especially to access the internal networks from external networks, unless a documented exception exists based on the use of a similarly effective control.

- **Assess third-party service providers, especially including their use of cloud computing**. Risks associated with the use of third-party service providers should be assessed, and service providers should themselves be required to have and follow security procedures. In light of the prevalence of use of third party service providers by retirement plans, the DOL published a separate set of DOL guidance regarding their use, which may be found here.

- **Conduct annual cybersecurity awareness training**. The DOL suggests conducting an annual cybersecurity awareness to educate each employee to recognize attacks, prevent incidents, and guard against ID theft.

- **Implement a secure system development life cycle (SDLC) program**. This program is intended to ensure that penetration testing, code review and other security assurance activities are an integral part of the system development process.

- **Implement a business resiliency program to address business continuity, disaster recovery and incident response**. The DOL views "business resilience" as the ability to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and data. A key aspect of this program is the establishment of business continuity principles specifically tailored to the retirement plan.

- **Encrypt sensitive data**. The plan administrator should implement standards for encryption data that are stored and for data that are transmitted.

- **Have strong technical controls that implement best security practices**. Hardware, software and firmware should be current and kept up to date, with routine data backup and patch management.

- **Be responsive to cybersecurity incidents or breaches**. These actions may include informing law enforcement, notifying insurers, investigating the incident and fixing the problem.

We expect that these topics will form the basis of any DOL inquiry of a retirement plan, with a particular focus on the selection and ongoing monitoring of third-party service providers. Retirement plan administrators should use these DOL publications, along with other reputable cyber readiness resources, in assessing strengths and weaknesses in this key area.

Lawrence K. Cagney
Partner, New York
+1 212 909 6909
lkcagney@debevoise.com

Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com

Jonathan F. Lewis
Partner, New York
+1 212 909 6916
jflewis@debevoise.com

Jim Pastore
Partner, New York
+1 212 909 6793
jjpastore@debevoise.com

Johanna N. Skrzypczyk
Counsel, New York
+1 212 909 6291
jnskrzypczyk@debevoise.com