NOW + NEXT

DATA PRIVACY & CYBERSECURITY ALERT | NIXON PEABODY LLP

JUNE 23, 2021

Well that was fast: The Department of Labor commences cybersecurity audit activity

By Jenny L. Holmes

In April, the Department of Labor (DOL) issued its first guidance on cybersecurity practices for ERISA retirement plans. The guidance, which was largely in response to a U.S. Government Accountability Office report urging the DOL to issue cybersecurity recommendations, establishes the DOL's minimum expectations for addressing cybersecurity risks.

The guidance was issued in three parts: (i) Cybersecurity Program Best Practices; (ii) Tips for Hiring a Service Provider with Strong Cybersecurity Practices; and (iii) Online Security Tips. While all three parts of the guidance include tips and best practices, plans must make sure their practices and procedures are memorialized.

The first two parts of the guidance intend to help plan sponsors manage cybersecurity risks, including how to prudently select service providers. The Cybersecurity Program Best Practices offers twelve action items plan sponsors and plan service providers should do. This includes having a formal, well-documented cybersecurity program, conducting annual risk assessment, and implementing strong controls to protect the data. The third piece provides tips for plan participants and beneficiaries to reduce the risk of loss, such as using unique passwords and multi-factor authentication.

Generally, when the DOL or other regulators issue guidance like this, we would not expect to see audit activity for at least a year or two. However, we are already aware of several investigations that the DOL has commenced regarding cybersecurity practices. We are sharing a sample of requested documentation in one such investigation below.

Cybersecurity is not infallible. Incidents will happen. What's important—and what we believe the DOL will want to see—is the effort to prioritize cybersecurity. And given the recent audit activity, creating (or reviewing) your comprehensive cybersecurity program should be done sooner rather than later.

Example DOL audit questions:

- 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 security risk assessment reports
- All security control audit reports, audit files, penetration test reports and supporting documents, and any other third-party cybersecurity analyses
- All documents and communications describing security reviews and independent security assessments of the assets or data of the plan stored in a cloud or managed by service providers
- All documents describing any secure system development life cycle (SDLC) program, including penetration testing, code review, and architecture analysis
- All documents describing security technical controls, including firewalls, antivirus software, and data backup
- All documents and communications from service providers relating to their cybersecurity capabilities and procedures
- 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

Please note that you may need to consult not only with the sponsor of the plan, but with the service providers of the plan to obtain all documents responsive to these requests. If you are unable to produce documents responsive to any of the forgoing, please specify the requests and the reasons for the non-production.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

- Jenny L. Holmes, 585-263-1494, jholmes@nixonpeabody.com
- Eric Paley, 585-263-1012, epaley@nixonpeabody.com