Reinhart

Department of Labor Provides Cybersecurity Guidance for Stakeholders of ERISA-Covered Plans

For the first time, the U.S. Department of Labor's (DOL) Employee Benefits Security Administration (EBSA) has provided guidance on cybersecurity practices for ERISA-covered benefit plans and their plan sponsors, fiduciaries, service providers, participants and beneficiaries. With ERISA-covered plans holding trillions of dollars in assets and maintaining volumes of personal information on behalf of participants, the guidance serves as a warning from the DOL that plans cannot ignore the cybersecurity threats they face while operating in an increasingly electronic environment. The DOL also indicated that the guidance is meant to complement its recent regulations on electronic recordkeeping and delivery of disclosures to participants.

Released on April 14, 2021, the guidance comes in three publications, which the DOL indicates are meant to help plan sponsors, fiduciaries, service providers and participants safeguard plan assets, protect personal information and manage cybersecurity risk.

Cybersecurity Program Best Practices

Aimed at plan fiduciaries, recordkeepers and other service providers responsible for plan IT systems and data, this guidance details the best practices to help organizations mitigate cybersecurity risk.

1. Have a formal, well-documented cybersecurity program
2. Conduct prudent annual risk assessments
3. Obtain reliable annual third-party audits of security controls
4. Clearly define and assign information security roles and responsibilities
5. Create and maintain strong access control procedures
6. Ensure assets or data stored in a cloud or managed by a service provider are subject to appropriate security reviews and independent security assessments
7. Conduct annual cybersecurity awareness training for all personnel and updated as necessary to reflect risks identified in the most recent risk assessment
8. Implement and maintain a secure System Development Life Cycle (SDLC) program to ensure any in-house applications are developed with security in mind

POSTED:

Apr 22, 2021

RELATED PRACTICES:

Employee Benefits
https://www.reinhartlaw.com/practices/employee-benefits

RELATED SERVICES:

Data Privacy and Cybersecurity
https://www.reinhartlaw.com/services/data-privacy-and-cybersecurity

RELATED PEOPLE:

Collin S. Weyers
https://www.reinhartlaw.com/people/collin-weyers

Justin P. Musil
https://www.reinhartlaw.com/people/justin-musil

9. Maintain a business resiliency program addressing the following components: business continuity, disaster recovery and incident response plans
10. Encrypt sensitive data at rest and in transit
11. Have strong technical controls implementing best security practices (*e.g.*, routine software updates and data backups)
12. Respond appropriately to cybersecurity incidents and breach (*e.g.*, investigating the incident and notifying law enforcement and insurers)

The DOL also advises plan fiduciaries to consider these best practices when hiring and monitoring services providers.

Tips for Hiring a Service Provider with Strong Cybersecurity Practices

Aimed at sponsors and fiduciaries of 401(k) and other pension plans, this guidance provides recommendations for selecting and monitoring service providers that follow strong cybersecurity practices. Many of these recommendations are consistent with those listed in the ERISA Advisory Council's 2016 report titled *Cybersecurity Considerations for Benefit Plans*.

The DOL guidance recommends that plan sponsors and fiduciaries:

- Evaluate vendors' information security standards, practices and policies, and audit results, and compare them to the industry standards adopted by other institutions
- Ask the vendor how it validates its cybersecurity practices
- Evaluate the vendor's track record in the industry, including breach response, litigation and agency enforcement actions
- Determine if the vendor has appropriate insurance to cover losses and liabilities arising from a breach, security incident or other event
- Seek contract provisions which:
  - provide the right to review audit results and other materials demonstrating compliance with security standards;
  - require vendors to regularly obtain third party audits to determine compliance with security standards, policies and procedures;
  - provide clear restrictions regarding the use, disclosure and safeguarding of plan data;
  - require notification of, and cooperation regarding, security incidents and breaches affecting plan data;
  - require vendor compliance with applicable privacy, security and record

retention and destruction laws; and
- require appropriate insurance, such as cyber liability, professional liability and fidelity bond coverage

Online Security Tips

Addressed to plan participants and beneficiaries, this guidance suggests steps to undertake to reduce the risk of fraud and loss to 401(k) and other individual retirement accounts. The DOL recommends a number of good cyber hygiene practices, including:

- Setting up and routinely monitoring online accounts;
- Using strong and unique passwords;
- Using multifactor authentication (MFA) for logins;
- Keeping personal contact information and accounts current;
- Avoiding free Wi-Fi networks;
- Recognizing common warning signs of phishing attacks;
- Using antivirus and anti-malware software;
- Keeping applications and software up to date; and
- Knowing how to report identity theft and cybersecurity incidents.

For more information on good cyber hygiene practices while working remotely, please see our previously published articles: "Beware of Cybersecurity Attackers Taking Advantage of Coronavirus Uncertainty" and "Beware of Email Scammers During the Coronavirus Outbreak."

If you have questions or require further assistance, please do not hesitate to contact your Reinhart attorney or any member of Reinhart's Data Privacy and Cybersecurity Group.