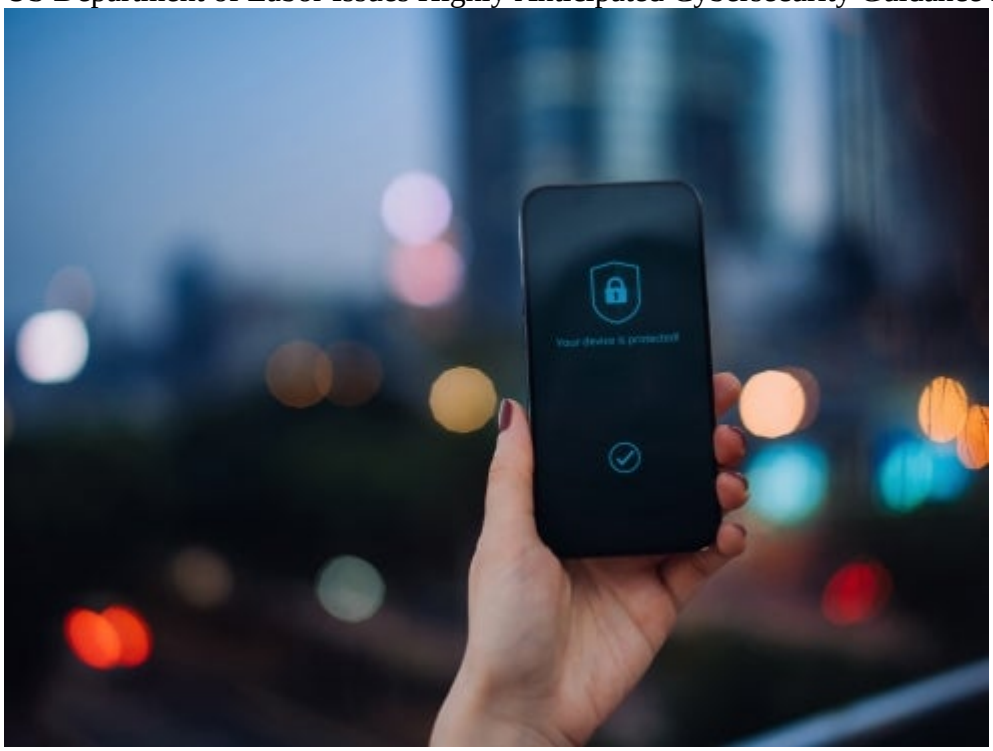
Updates
April 22, 2021
US Department of Labor Issues Highly Anticipated Cybersecurity Guidance for ERISA Plans



On April 14, 2021, the U.S. Department of Labor (DOL) released three-part guidance on cybersecurity issues for employee benefit plans, marking its first significant commentary on the issue since its comprehensive but nonbinding report in late 2016. The DOL's guidance arrives amidst an increase in high-profile lawsuits arising out of retirement plan participants' claims that plan sponsors, responsible fiduciaries, and service providers failed to adequately protect retirement accounts against cybersecurity threats. Given the increased threat of cybersecurity attacks in general and the potential vulnerability of approximately $9.3 trillion in benefit plan assets (per DOL estimation), ERISA plan sponsors, responsible fiduciaries, and participants have eagerly awaited formal DOL guidance on this issue. This update provides a detailed examination of the DOL's three-part cybersecurity guidance for ERISA plans as well as a summary of practical implications for plan sponsors and responsible fiduciaries.

DOL Guidance on Cybersecurity

Tips for Plan Sponsors and Responsible Fiduciaries on Hiring Service Providers With Strong Cybersecurity Practices. The DOL developed a list of the following six tips that plan sponsors and responsible fiduciaries should follow in fulfilling their duties under ERISA's requirements to prudently select and monitor ERISA plan service providers:

1. Requesting the service provider's security practices and protocols and comparing these systems to industry standards adopted by other financial institutions.
2. Inquiring as to how the service provider validates its security controls, including by securing a contractual right to review security system audit results.

3. Evaluating the service provider's information security track record, including by reviewing publicly available information on security incidents and related litigation.
4. Confirming any recent security breach issues and related responses.
5. Confirming whether the service provider has sufficient cybersecurity and identity theft insurance coverage to meet the needs of the plan and its participants.
6. Incorporating ongoing cybersecurity compliance requirements into service agreements as well as other contractual requirements, such as (a) third-party audit requirements; (b) limitations on use and disclosure of confidential information; (c) prompt notification of cybersecurity breaches; (d) record retention policies in compliance with applicable law; and (e) adequate cybersecurity, identity theft, and breach insurance coverage (whether as a stand-alone policy or as a rider to the service provider's existing errors and omission liability insurance policies).

Cybersecurity Program Best Practices for Plan Recordkeepers and Service Providers. The DOL further provided a detailed description of twelve best practices that should be followed by plan recordkeepers and other service providers responsible for plan-related IT systems and data, as well as for plan fiduciaries in making prudent decisions when selecting service providers. The DOL's best practice cybersecurity recommendations for plan recordkeepers and relevant service providers include (in brief):

1. Having a well-documented cybersecurity program capable of identifying, assessing, protecting against, recovering from, and appropriately disclosing both internal and external cybersecurity threats to the confidentiality, integrity, or availability of stored nonpublic information. The cybersecurity program should implement formal policies designed to limit and counteract cybersecurity threats (e.g., access management, incident response, and security control policies and procedures).
2. Conducting an annual risk assessment designed to identify information security threats and result in the revision of cybersecurity controls as needed to respond to existing and emerging threats.
3. Engaging an independent third-party auditor to assess the security controls and document the correction of any weaknesses on at least an annual basis.
4. Identifying a chief information security officer with sufficient expertise and necessary credentials to establish and maintain the cybersecurity program.
5. Implementing strong access control procedures that limit access to information systems and sensitive plan and participant data through authorization procedures and identity authentication controls.
6. Engaging in regular security reviews of cloud storage providers' and other third-party data storage providers' information systems, including through the use of third-party independent security assessments of such systems.
7. Conducting annual cybersecurity awareness trainings for all personnel, with particular emphasis on risks identified in the most recent risk assessment.
8. Implementing a secure system development lifecycle program designed to evaluate the security of any applications developed and used in-house through periodic vulnerability and penetration testing for all customer-facing applications (and data maintained therein).
9. Developing a business resiliency program that effectively addresses business continuity, disaster recovery, and incident response programming in each circumstance to ensure the safeguarding and ongoing availability of people, assets, and data on the occurrence of a cybersecurity event or disaster.
10. Encrypting all nonpublic plan and participant information at all times, including when stored and in transit.
11. Implementing strong technical controls for hardware, software, or firmware components of the information systems (e.g., regular updates to system components).
12. Responding appropriately to cybersecurity incidents or breaches in order to protect the plan and its participants, including by notifying law enforcement and any relevant insurers, investigating the incident, informing affected plans and participants of steps to take to prevent or reduce injury, and fixing problems that gave rise to the incident or breach.

Online Security Tips for Retirement Plan Participants. The DOL also issued guidance providing tips for participants to reduce the risk of fraud and loss to their retirement accounts. These tips include many now-standard methods for protecting personal assets and information while online, such as routinely monitoring online accounts, using strong and unique passwords, using multifactor authentication when available, updating personal contact information, closing unused accounts, being wary of free Wi-Fi and phishing attacks, using updated anti-virus software, and knowing how to report identity theft and cybersecurity incidents.

Practical Implications for ERISA Plan Sponsors and Responsible Fiduciaries

The DOL's guidance on cybersecurity issues for ERISA plans carry practical implications for plan sponsors and responsible fiduciaries, including the following highlights:

- Though the DOL describes its guidance as "tips" and "best practices," responsible fiduciaries are subject to ERISA's prudent selection and monitoring standards with respect to engaging and retaining recordkeepers and other service providers. Responsible fiduciaries, therefore, should consider the DOL's tips for provider selection in their compliance efforts.
- The DOL's guidance likely indicates an increased focus on cybersecurity issues in DOL enforcement actions, so responsible fiduciaries should evaluate the DOL's tips in preparing for potential review or investigation. The DOL's guidance may also spur litigation and move the needle on the criteria for determining whether responsible fiduciaries acted prudently.
- Though the DOL's guidance on cybersecurity insurance relates to service providers' coverage, plan sponsors and responsible fiduciaries should confirm whether existing fiduciary liability insurance will adequately cover cybersecurity issues. If not, plan sponsors and responsible fiduciaries should discuss with insurers the possibility of adding supplemental coverage to address cybersecurity-related loss.
- Plan sponsors and responsible fiduciaries should consider addressing both the DOL's best practices for providers and tips for provider selection in vendor procurement processes, including within internal trainings for personnel involved in the vendor selection process.
- Plan sponsors and responsible fiduciaries for plans of all sizes should treat the DOL's best practices for providers as a checklist for reviewing their own cybersecurity readiness with respect to internal plan administration. The lack of security controls at the plan sponsor level can lead to losses that arguably cannot be prevented at the provider level. Sponsors and responsible fiduciaries may need to consider engaging third-party consultants specializing in cybersecurity issues to promote readiness and the security of plan participants' assets and information. Given the increasing regularity of cybersecurity incidents, plan sponsors and responsible fiduciaries may need to act promptly to conduct this review and remedy any issues identified in order to reduce the risk of losses to ERISA plan participants.
- The DOL's guidance largely mirrors guidance issued by the U.S. Department of Health and Human Services with respect to the security controls under the HIPAA Security Rule and the requirements thereunder. Plan sponsors and responsible fiduciaries conducting a review of their cybersecurity controls may be able to leverage policies, procedures, and controls applicable to group health plans governed by HIPAA, or, on finding those controls insufficient, engage in a uniform remediation program to improve cybersecurity controls for all ERISA plans.

Authors

Explore more in

Employee Benefits & Executive Compensation Corporate Law Labor & Employment Privacy & Security Public Companies

Related insights

Update

Two Tools for Trump To Dismantle Biden-Era Rules: the Regulatory Freeze and the Congressional Review Act

Update

The FY 2025 National Defense Authorization Act: What's New for Defense Contractors