VOLUME 25, NUMBER 2
JUNE 2021

THE ECFC
FLEX REPORTER

US Department of Labor Announces New Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Record-Keepers and Plan Participants

---

The Employee Benefit Security Administration ("EBSA") of the U.S. Department of Labor ("DOL") announced on April 14, 2021 new cybersecurity guidance applicable to Plan Sponsors, Plan Fiduciaries, Record Keepers and Plan Participants on best practices for maintaining cybersecurity. The News Release provides that "[t]his guidance is directed at plan sponsors and fiduciaries regulated by the Employee Retirement Income Security Act, and plan participants and beneficiaries."

If one reads the News Release and subsequent guidance by itself one would not be aware that the guidance was preceded by what appears to be extensive discussions between the DOL and the United States Government Accountability Office ("GAO") about the timing and content of that guidance. The GAO released a report, titled "DEFINED CONTRIBUTION PLANS, Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans, (GAO-21-25, February 2021) to Congressional requestors available at (https://www.gao.gov/assets/gao-21-25.pdf).

This Alert will review the GAO Report for context and background, and then discuss the DOL's first foray into guidance concerning cybersecurity in the context of ERISA-covered employee benefit plans. As an aside, two terms that appear in the February 2021 Report that are important are:

- **"PII" or "personally identifiable information"** is "any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, or Social Security number; and other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information."

- **"Plan asset data"** is "sensitive information that is associated with a participant's retirement assets, such as their retirement account number and bank account information."

Starting on Page 30 of the February 2021 GAO Report, there is a statement that "we (GAO) are making two recommendations to DOL:

"The Secretary of Labor should formally state whether cybersecurity for private sector employer-sponsored defined contribution retirement plans is a plan fiduciary responsibility under ERISA. (Recommendation 1)

"The Secretary of Labor should develop and issue guidance that identifies minimum expectations for mitigating cybersecurity risks that outline the specific requirements that should be taken by all entities involved in administering private sector employer-sponsored defined contribution retirement plans. (Recommendation 2)."

The DOL did not directly respond to the first recommendation and effectively accepted the second recommendation.

In the apparent chain of events, the DOL provides in a News Release issued on April 14, 2021 that is describing the guidance that comes in three parts:

- "**Tips for Hiring a Service Provider**: Helps plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities, as ERISA requires.
- "**Cybersecurity Program Best Practices**: Assists plan fiduciaries and record-keepers in their responsibilities to manage cybersecurity risks.
- **"Online Security Tips:** Offers plan participants and beneficiaries who check their retirement accounts online basic rules to reduce the risk of fraud and loss."

The issuance of this guidance does not reference the February 2021 GAO Report even though it appears to be directly responsive to it. The guidance is an important step towards helping to protect retirement benefits and personal information. The guidance "complements EBSA's regulations on electronic records and disclosures to plan participants and beneficiaries. EBSA issued important guidance concerning cybersecurity in relation to ERISA-covered employee benefit plans, with separate items directed chiefly to service providers, fiduciaries, and participants and beneficiaries.

The form of the DOL guidance is unusual in that it was issued, effectively, as three best practice guides rather than as proposed regulations or other forms of guidance which we are used to seeing. To the extent that there is DOL enforcement of these guidelines or private litigation based on the contents of this guidance, it should be interesting to see how the guidance will be stylized and relied upon.

This Article will now expand upon each part of the guidance briefly described above.

"Tips for Hiring a Service Provider with Strong Cybersecurity Practices":

Helps plan sponsors and fiduciaries of 401(k) and other types of pension plans to prudently select a service provider with strong cybersecurity practices and monitor their activities, as ERISA requires.

The Tips are intended as guidance for plan sponsors and plan fiduciaries. Tips for these fiduciaries include:

1. "Ask about the service provider's information security standards, practices, policies and audit results and compare them to the industry standards adopted by other financial institutions.
2. "Ask the service provider how it validates its practices, and what level of security standards it has met and implemented.
3. "Evaluate the service provider's track record in the industry, including public information regarding information security incidents, other litigation, and legal proceedings related to the vendor's services.

4. "Ask whether the service provider has experienced past security breaches; what happened; and how the service provider responded.

5. "Find out if the service provider has any insurance policies that would cover losses caused by cybersecurity and identity theft breaches (including breaches caused by" both internal and external threats.

6. "…https://www.gao.gov/assets/gao-21-25.pdf). Make sure that the contract with the service provider requires ongoing compliance with cybersecurity and information security standards..."

The DOL guidance also suggests trying to include certain provisions in the contract that would require ongoing compliance with cybersecurity and information security standards, such as:

1. "Information Security Reporting.

2. "Clear provisions on the use and sharing of Information and Confidentiality.

3. "Notification of Security Breaches.

4. "Compliance with Records Retention and Destruction, Privacy, and Security laws; and

5. "Insurance" - Requiring various types of insurance, including but not limited to cyber liability and privacy breach insurance and understand the terms and limits of the coverage.

"Cybersecurity Program Best Practices":

EBSA has prepared Best Practices for recordkeepers and other service providers responsible for plan-related IT Systems and data.

"The Employee Benefits Security Administration has prepared the following best practices for use by recordkeepers and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire. Plans' service providers should:

1. "Have a formal, well documented cybersecurity program.

2. "Conduct prudent annual risk assessments.

3. "Have a reliable annual third-party audit of security controls.

4. "Clearly define and assign information security roles and responsibilities.

5. "Have strong access control procedures.

6. "Ensure that any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.

7. "Conduct periodic cybersecurity awareness training.

8. "Implement and manage a secure system development life cycle (SDLC) program.

9. "Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.

10. "Encrypt sensitive data, stored and in transit.

11. "Implement strong technical controls in accordance with best security practices.

12. "Appropriately respond to any past cybersecurity incidents."

The concepts inherent in the "Cybersecurity Program Best Practices" should be incorporated in the actual contract for services between the Plan/Plan Sponsor and the Service Provider. These concepts can be used as the framework for the compliance portions of the Service Agreement.

"Online Security Tips"

These tips are primarily intended for Plan Participants. However, they can be helpful when formulating the Request for Proposal for a new service provider for the Plan to develop minimum service requirements for the Service Provider.

They are as follows:

1. "Register, Setup and Routinely Monitor Online Accounts;

2. "Use Strong and Unique Passwords;

3. "Use Multi-Factor Authentication:

4. "Keep Personal Contract Information Current;

5. "Close or Delete Unused Accounts;

6. "Be Wary of Free Wi-Fi;

7. "Beware of Phishing Attacks;

8. "Use Antivirus Software and Keep Apps and Software Current; and

9. "Know How to Report Identity Theft and Cybersecurity Incidents."

VOLUME 25, NUMBER 2
JUNE 2021

THE ECFC
FLEX REPORTER

SUMMARY

Even though this Article is a summary of Cybersecurity Best Practices, they are important concepts with which to be familiar when administering an employee benefit plan. The standards for welfare plans are not as well developed as are those for 401(k) Plans. However, one should be aware of welfare plan security rules, to the extent that they are developed, and implement them, to the extent possible.