GAO@100

Highlights

Highlights of GAO-21-25, a report to congressional requesters

February 2021

DEFINED CONTRIBUTION PLANS

Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans

Why GAO Did This Study

Cyber attacks against information systems (IT) are perpetuated by individuals or groups with malicious intentions, from stealing identities to appropriating money from accounts. DC plans, which allow individuals to accumulate tax-advantaged retirement savings, increasingly rely on the internet and IT systems for their administration. Accordingly, the need to secure these systems has become paramount. Ineffective data security controls can result in significant risks to plan data and assets. In 2018, DC plans enrolled 106 million participants and held nearly $6.3 trillion in assets, according to DOL.

This report examines (1) the data that sponsors and providers exchange during the administration of DC plans and their associated cybersecurity risks, and (2) efforts to assist sponsors and providers to mitigate cybersecurity risks during the administration of DC plans. GAO interviewed key entities involved with DC plans, such as sponsors and record keepers, DOL officials and industry stakeholders; and reviewed relevant federal laws, regulations, and guidance.

What GAO Recommends

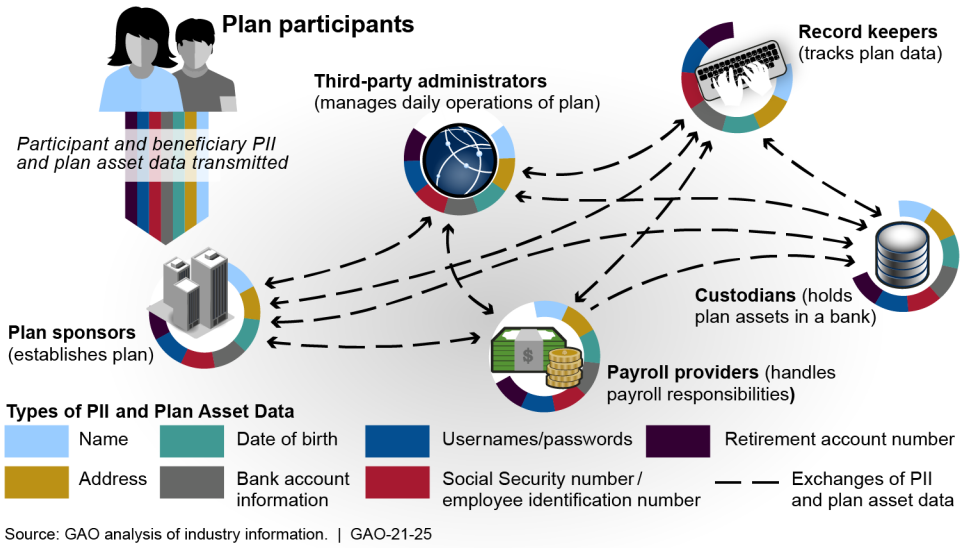
GAO is making two recommendations to DOL to formally state whether it is a fiduciary's responsibility to mitigate cybersecurity risks in DC plans and to establish minimum expectations for addressing cybersecurity risks in DC plans. DOL agreed with GAO's second recommendation but did not state whether it agreed or disagreed with the first one. GAO believes both recommendations are warranted.

View GAO-21-25. For more information, contact Tranchau "Kris" Nguyen at (202) 512-2660 or nguyentt@gao.gov; or Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

In their role administering private sector employer-sponsored defined contribution (DC) retirement plans, such as 401(k) plans, plan sponsors and their service providers—record keepers, third party administrators, custodians, and payroll providers—share a variety of personally identifiable information (PII) and plan asset data among them to assist with carrying out their respective functions (see figure). The PII exchanged for DC plans typically include participant name, Social Security number, date of birth, address, username/password; plan asset data typically includes numbers for both retirement and bank accounts. The sharing and storing of this information can lead to significant cybersecurity risks for plan sponsors and their service providers, as well as plan participants.

Data Sharing Among Plan Sponsors and Service Providers in Defined Contribution Plans



Source: GAO analysis of industry information. | GAO-21-25

Federal requirements and industry guidance exist that could mitigate cybersecurity risks in DC plans, such as requirements that pertain to entities that directly engage in financial activities involving DC plans. However, not all entities involved in DC plans are considered to have such direct engagement, and other cybersecurity mitigation guidance is voluntary. Federal law nevertheless requires plan fiduciaries to act prudently when administering plans. However, the Department of Labor (DOL) has not clarified fiduciary responsibility for mitigating cybersecurity risks, even though 21 of 22 stakeholders GAO interviewed expressed the view that cybersecurity is a fiduciary duty. Further, DOL has not established minimum expectations for protecting PII and plan assets. DOL officials told GAO that the agency intends to issue guidance addressing cybersecurity-related issues, but they were unsure when it would be issued. Until DOL clarifies responsibilities for fiduciaries and provides minimum cybersecurity expectations, participants' data and assets will remain at risk.