Congress of the United States

Washington, DC 20510

February 12, 2019

The Honorable Gene Dodaro
Comptroller General
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Dodaro:

We write to request the U.S. Government Accountability Office (GAO) examine the cybersecurity of the private retirement system. Retirement savings held in defined contribution plans, like 401(k) plans, have grown steadily in recent years, reaching over $5 trillion in 2017. These savings, the new methods of connecting savers with their retirement plans, and the digital interactions between the plans and their service providers hold great promise for both increasing financial literacy and improving financial security for retirement. At the same time, they are also a tempting target for criminals who could hack into plans and individuals' accounts to access information, commit identity fraud, and steal retirement savers' nest eggs. It is important that workers and retirees know their savings are in fact safe, and that a cyberattack will not throw the retirement they have spent years working and planning for into jeopardy.

Most plan sponsors and their service providers have moved account information online to increase participant access to their accounts. Yet while the digitization and online storage of account information provides many advantages, it also creates new risks for plans and participants, as recent data breaches at Equifax and other financial service providers and institutions demonstrate. The Financial Services Information Sharing and Analysis Center (FS-ISAC) was established to meet these challenges and to strengthen the collective cybersecurity of the financial industry by promoting the exchange of information about cyberthreats and vulnerabilities. Last year, FS-ISAC and the SPARK Institute created the Retirement Industry Council (RIC) in order to provide similar information sharing and threat intelligence to its members in the retirement industry as they extend beyond the financial industry and the purview of the FS-ISAC. Despite the creation of these forums, the cybersecurity safeguards, risks, and liabilities for plan sponsors and participants remain ill-defined, especially with regard to major data breaches or advanced persistent threats.

Under current law, retirement plan fiduciaries are responsible for designing and administering plans in the best interests of plan participants. Current law, however, does not address a number of questions related to cybersecurity, and retirement plans fall within a patchwork of federal and state laws and regulations. Given the risk of cyberattacks targeting plan data and retirement savings, and the importance of deterring such attacks(both to protect savings and to encourage ongoing participation in workplace retirement savings plans),we would like GAO to address the following questions:

1. What potential threats do cyberattacks pose to U.S. retirement plan data and ultimately to plan participants' financial well-being?

2. Given these threats, what are plan sponsors doing to ensure that, as plan fiduciaries, they are taking steps to protect plan data and plan participants? To what extent have plan sponsors and recordkeepers thoroughly assessed security and privacy risks and adopted appropriate measures to ensure that plan data, participants' personal information, and participants' retirement savings are adequately safeguarded?

3. What are plan service providers doing to ensure they are taking the necessary steps to protect plan data and plan participants from these threats? When a data breach does occur, what are the circumstances and the processes under which plan service providers disclose a breach to a plan sponsor?

4. To what extent do federal laws and regulations require plan sponsors, record keepers, and other retirement plan service providers to protect plan data and plan participants from these risks?

5. In the event of a data breach, what steps should plan sponsors be required to take to protect plan participants?

6. Do current ERISA bonding requirements sufficiently insure against these risks? Would requiring cybersecurity insurance in addition to existing ERISA bonding requirements mitigate some of these risks? If so, are these policies widely available? Are they cost prohibitive? If Congress were to contemplate such a requirement, what would a proper bond amount be and which parties should be required to be bonded?

7. To the extent that cybersecurity insurance is not sufficiently available on the commercial market, should Congress consider establishing a federal cybersecurity insurer?

8. To what extend do the National Cyber Strategy and relevant federal agencies' policies prioritize working with the private sector to deter potential cyberattacks involving participants' retirement savings?

9. What are retirement plan sponsors, industry stakeholders, and government regulators in other countries doing to prevent cyberattacks involving retirement savings, and what lessons, if any, should the U.S. take from them?

10. What are possible legislative or regulatory options to bolster the protection of both the data and accounts of retirement savers?

We appreciate GAO's assistance with this study. If you have any questions concerning this request, please contact Kendra Isaacson, Senior Pensions Counsel for the Senate HELP Committee, at (202) 224-6572, and Kevin McDermott, Senior Labor Policy Advisor for the House Education & Labor Committee, at (202) 225-3725.

Thank you for your attention to this matter.

Sincerely,

ROBERT C. "BOBBY" SCOTT
Chairman, House Committee on Education & Labor

PATTY MURRAY
Ranking Member, Senate Committee on Health, Education, Labor & Pensions