United States Government Accountability Office

Report to Congressional Requestors

February 2021

DEFINED CONTRIBUTION PLANS

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

Accessible Version

GAO-21-25

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

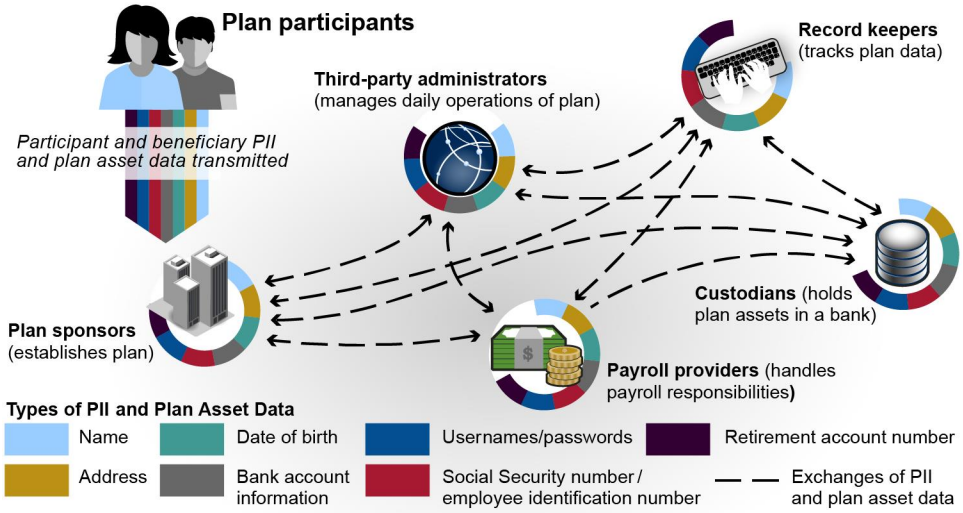
GAO is making two recommendations to DOL to formally state whether it is a fiduciary's responsibility to mitigate cybersecurity risks in DC plans and to establish minimum expectations for addressing cybersecurity risks in DC plans. DOL agreed with GAO's second recommendation but did not state whether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

Contents

Abbreviations

AICPA	American Institute of Certified Public Accountants
CISA	Cybersecurity and Infrastructure Security Agency
DB	defined benefit
DC	defined contribution
DOL	Department of Labor
EBSA	Employee Benefits Security Administration
ERISA	Employee Retirement Income Security Act of 1974, as amended
FS-ISAC	Financial Services Information Sharing and Analysis Center
FTC	Federal Trade Commission
GLBA	Gramm-Leach Bliley Act
IT	information technology
NIST	National Institute of Standards and Technology
PII	personally identifiable information
SOC	System and Organization Control
SPARK	Society of Professional Asset Managers and Recordkeepers Institute
TPA	third-party administrator

441 G St. N.W.
Washington, DC 20548

February 11, 2021

The Honorable Patty Murray
Chair
Committee on Health, Education, Labor, and Pensions
United States Senate

The Honorable Robert C. "Bobby" Scott
Chairman
Committee on Education and Labor
House of Representatives

The Honorable Margaret Wood Hassan
United States Senate

In 2019, the Federal Bureau of Investigation received nearly half a million complaints of suspected cyber crimes, with reported losses exceeding $3.5 billion.[1] Cyber attacks against information technology (IT) systems and applications are perpetrated by individuals and groups with malicious intentions including obtaining sensitive information, committing fraud, disrupting operations, and stealing money from accounts. Consequently, the security of IT systems and networks is essential to protecting private sector employer-sponsored retirement plans.[2] Conversely, ineffective cybersecurity controls[3] can create significant risks. These risks can result in the loss or theft of resources, such as retirement plan assets, and inappropriate access to and disclosure, modification, or destruction of retirement plan participants' sensitive information.

[1]Federal Bureau of Investigation, *2019 Internet Crime Report* (Washington, D.C.: February 2020).

[2]There are two predominant types of private sector employer-sponsored retirement plans in the United States: defined contribution plans and defined benefit plans. Both types of plans are described in the Background section of the report. The focus of this report is defined contribution plans.

[3]Cybersecurity controls are designed to ensure that (1) access to data is appropriately restricted; (2) physical access to sensitive computing resources and facilities is protected; (3) systems are securely configured to avoid exposure to known vulnerabilities; (4) duties are segregated among individuals; and (5) backup and recovery plans are adequate and tested to ensure the continuity of essential operations.

The Employee Retirement Income Security Act of 1974 established minimum standards and requirements intended to protect plan participants and beneficiaries in private sector employer-sponsored retirement plans.[4] However, since then, plan sponsors and their service providers have increasingly relied on the internet and IT systems to execute tasks required to administer these retirement plans. Further, plan sponsors may outsource the administration of retirement plans, including record keeping and other services, to third-party service providers, thus increasing the potential opportunities for malicious individuals to gain unauthorized access to accounts, participant personally identifiable information (PII),[5] and plan asset data.[6]

The increase in retirement savings and reliance by Americans on private sector employer-sponsored defined contribution (DC) retirement plans make protecting against cyber attacks a paramount issue for those involved with ensuring retirement security. From 1990 to 2018, the number of participants in these plans increased by about 180 percent and the amount of assets held in these plans increased more than seven-fold.[7] The most current data provided by the Department of Labor (DOL) show that as of 2018, 106 million people were participating in private sector employer-sponsored DC retirement plans with assets of nearly $6.3 trillion. In many cases, these funds are a participant's only savings

[4]See Pub. L. No. 93-406, 88 Stat. 829 (codified as amended in various sections of 26 and 29 U.S.C.)

[5]PII 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.

[6]For reporting purposes, we have defined "plan asset data" as sensitive information that is associated with a participant's retirement assets, such as their retirement account number and bank account information.

[7]See U.S. Department of Labor, Employee Benefits Security Administration, *Private Pension Plan Bulletin Historical Tables and Graphs 1975-2018* (Washington, D.C.: Forthcoming). DOL officials provided 2018 data from its latest report that is forthcoming.

for retirement, underscoring the importance of protecting these assets from cyber attacks.[8]

You asked us to review issues related to the cybersecurity of retirement plans. This report examines 1) what PII and plan asset data plan sponsors and service providers exchange during the administration of private sector DC retirement plans in the United States and the associated cybersecurity risks and 2) the extent to which federal or industry efforts require or assist with measures that plan sponsors and service providers can use to mitigate the cybersecurity risks facing private sector DC retirement plans in the United States.

To better understand what PII and plan asset data plan sponsors and service providers exchange during the administration of private sector DC retirement plans in the United States and the associated cybersecurity risks, we conducted semi-structured interviews with representatives from 13 key entities—two custodians, one payroll provider, two plan sponsors, five record keepers, and three third-party administrators (TPAs)—responsible for the administration of private sector employer-sponsored retirement plans.[9] To facilitate the selection of these entities, we worked with knowledgeable stakeholders in the retirement industry to identify and connect with companies willing to be interviewed for our review. We selected companies that varied in size based on the company's total amount of DC plan assets, and for record keepers, the total number of 401(k) plans. To further understand any potential risks associated with the exchange of data, we analyzed previous GAO work on this topic, and reviewed industry reports that described cybersecurity threats and risks. We also discussed potential cyber risks with six retirement industry stakeholders, including representatives from the ERISA Advisory Council; an attorney group that specializes in retirement; a financial sector group that specializes in sharing threat information; and two national organizations representing retirement industry stakeholders.

[8]In our prior work, we have described three main pillars that comprise the nation's retirement system: Social Security, employer-sponsored pensions or retirement savings plans, and individual savings. See GAO, *The Nation's Retirement System: A Comprehensive Re-Evaluation is Needed to Better Promote Future Retirement Security*, GAO-18-111SP (Washington, D.C.: Oct. 2017).

[9]In this report, we limited the scope of our review to the administration of private sector employer-sponsored DC retirement plans in the United States and to the cybersecurity risks present during the administration of these plans.

To understand the extent to which federal or industry efforts exist to require or assist plan sponsors and service providers in mitigating the cybersecurity risks facing private sector DC retirement plans in the United States, we reviewed and analyzed federal laws, regulations, and guidance. We also reviewed and analyzed industry reports, training materials, leading practices, and planning documents related to retirement plans and cybersecurity. We conducted interviews with agency officials from DOL, the Federal Trade Commission (FTC), the Department of Homeland Security, the Pension Benefit Guaranty Corporation, the U.S. Securities and Exchange Commission, and the Department of the Treasury as well as industry stakeholders to obtain their views on these federal and industry efforts.

We selected 34 industry stakeholders to interview for the second research objective based on their expertise in subjects related to retirement plans, the Employee Retirement Income Security Act of 1974, as amended, (ERISA), or cybersecurity. These 34 industry stakeholders included the six industry stakeholders interviewed for the first objective; officials from seven additional national organizations representing a range of entities, including plan sponsors, service providers, and participants; 10 additional attorneys and two academics who specialize in ERISA, retirement plans, or cybersecurity; representatives from six insurance companies that offer cyber insurance; and representatives from three retirement plan service providers. Further, we reviewed and analyzed documents obtained during these interviews for additional information on these efforts. Finally, we reviewed DOL's actions relative to cybersecurity for retirement plans and analyzed interview responses from selected plan sponsors and service providers and industry stakeholders related to cybersecurity risk mitigation in retirement plans.

For both research questions, we conducted a discussion group of about 40 representatives at the 2019 Society of Professional Asset Managers and Recordkeepers Institute (SPARK) Forum—a conference for leaders in the retirement industry— to discuss potential cybersecurity risks in retirement plans, federal or industry guidance currently being used to mitigate these potential risks, and what federal actions, if any, would be helpful to mitigate potential cyber risks for retirement plans.

We conducted this performance audit from May 2019 to February 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that

the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The two predominant types of private sector employer-sponsored retirement plans that exist in the United States are DC plans and defined benefit (DB) plans. DC plans, the focus of this report, are employer-sponsored account-based retirement plans, such as 401(k) plans, that allow individuals to accumulate tax-advantaged retirement savings in an individual account from employee and employer contributions, and the investment returns earned on the account. In contrast, a DB plan is an employer-sponsored retirement plan that traditionally promises to provide a benefit for the life of the participant, based on a formula specified in the plan that typically takes into account factors such as an employee's salary, years of service, and age at retirement.

In the past, many employers offered DC plans as a supplemental way for employees to save for retirement in addition to their primary DB plan. However, we have reported that DC plans have in recent decades become the dominant employer-sponsored retirement plan type in the private sector.[10] Retirement experts have posited a variety of reasons for employers' switch to DC plans. One reason experts have cited was the introduction of 401(k) accounts in 1978, which they credit with fostering the adoption of account-based plans by sanctioning the use of employee salary deferrals as a source of contributions. Unlike DB plans that are employer funded, a 401(k) plan allows individuals to accumulate retirement savings in an individual account based on employee and/or employer contributions, and the investment returns (gains and losses) earned on the account. Under a 401(k) plan, employees often are responsible for managing the investments of their accounts and choosing from investment options offered by the plan.[11] There is no comprehensive

[10]See GAO-18-111SP.

[11]In a DB plan, plan officials manage the investment and the employer is responsible for ensuring that the amount it has put in the plan plus investment earnings will be enough to pay the promised benefit. In a DC plan, there is no promised benefit; the benefit depends on contributions made by the employee and/or the employer, performance of the account's investments, and fees charged to the account.

federal guarantee of 401(k) plan benefits lost, for example, due to poor investment decisions by the employee or other reasons, such as theft.[12]

DOL's Employee Benefits Security Administration (EBSA) is the agency responsible for administering and enforcing the fiduciary responsibility and reporting and disclosure provisions of Title I of ERISA.[13] EBSA issues guidance, including field assistance bulletins and technical releases, to assist plan administrators with managing retirement plans.[14] ERISA also grants DOL the authority to issue regulations to carry out these provisions.[15]

The Administration of Defined Contribution Plans

Administering a DC plan can be complex and involve several entities. Typically, an employer—referred to as a plan sponsor—offers a DC plan to its employees and contracts with service providers to help administer specific aspects of the plan. Figure 1 describes the roles of several selected entities in administering DC retirement plans. For reporting purposes, we have defined "service providers" to include record keepers, third-party administrators, payroll providers, and custodians.[16]

[12]However, ERISA allows DOL and plan participants and beneficiaries to bring a civil action for various reasons, including for breach of fiduciary duty. See 29 U.S.C. § 1132.

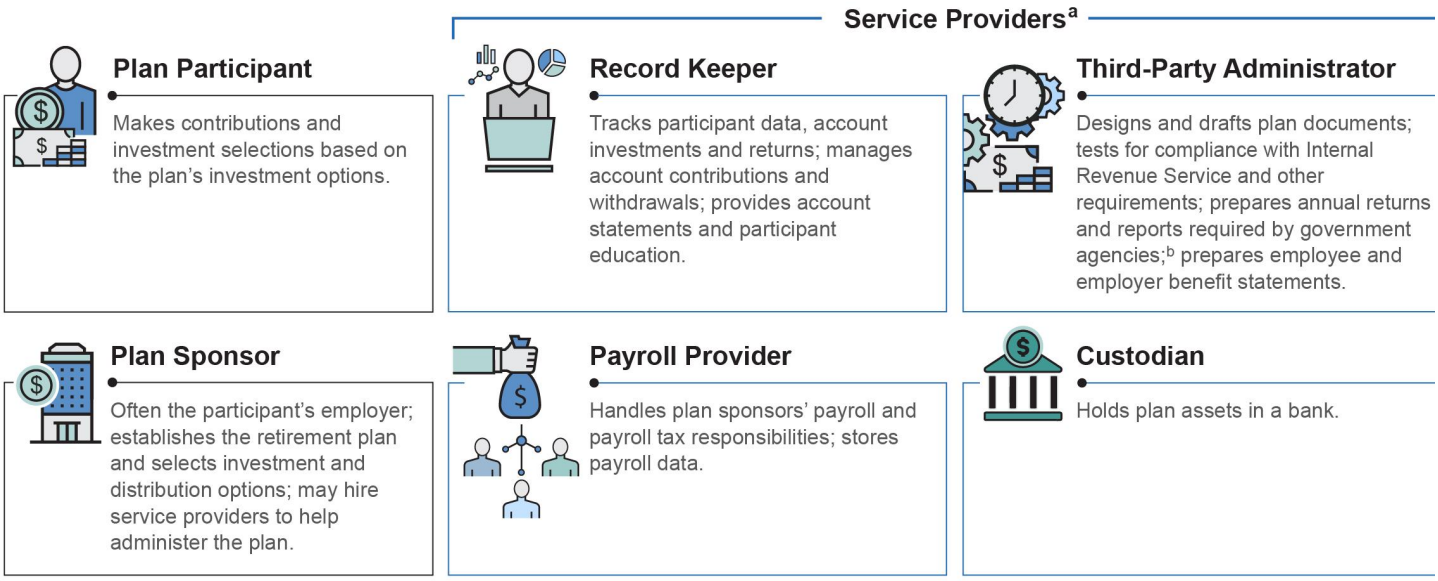
[13]See 29 U.S.C. §§ 1021-1031 and 1101-1114. Title I of ERISA generally provides requirements for private sector employers sponsoring retirement plans.

[14]Field Assistance Bulletins provide guidance in response to questions that have arisen in field operations and may include transition enforcement relief that permits employers, plan officials, service providers and others time to respond to new laws or regulations, according to EBSA.

[15]See 29 U.S.C. § 1135.

[16]Additional entities are involved in the administration of DC plans, such as broker/dealers, investment advisers, and fund managers. They are not discussed in this report.

Figure 1: Roles of Selected Entities in the Administration of a Defined Contribution Plan



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

[a]Entities can take on multiple roles during the administration of a defined contribution retirement plan, some of which are not described here. This figure is not meant to be an exhaustive description of the entities' functions or the entities involved as there are other entities that may be involved with the administration of a defined contribution plan.

[b]Plan sponsors often use third-party administrators to help them meet their federal reporting and disclosure requirements.

Fiduciary Responsibilities under ERISA

Under ERISA, a fiduciary generally includes any person who:

- exercises any discretionary authority or control over plan management;
- exercises any authority or control over the management or disposition of plan assets;
- renders investment advice with respect to plan money or property for a fee or other compensation; or

- has discretionary authority or responsibility for plan administration.[17]

ERISA also sets forth standards and rules for the conduct of plan fiduciaries. Among other things, ERISA requires fiduciaries to carry out their duties solely in the interest of plan participants and beneficiaries and with the same care and skill that a prudent person acting in a similar capacity would use.[18] Plan fiduciaries could include, for example, plan trustees, plan administrators (e.g., plan sponsors, record keepers, custodians, TPAs), or members of a plan's investment committee. Employers who maintain plans, often the plan sponsors, are typically fiduciaries with respect to performing certain functions, such as by serving as named fiduciaries or by exercising control over the management of the plan. Service providers may also be fiduciaries depending on the functions they perform.

Ensuring the Cybersecurity of the Nation Included on GAO's High Risk List Since 1997

We have previously reported that federal agencies and the nation's critical infrastructures,[19] including financial services, are dependent on information technology systems to carry out operations. The security of these systems and the data they use is vital to public confidence and national security, prosperity, and well-being. Because many of these systems contain vast amounts of PII, we have stated that agencies must protect the confidentiality, integrity, and availability of this information. In

[17]See 29 U.S.C. § 1002(21)(A). Employer-sponsored retirement plans have one or more "named fiduciaries" with the authority to control and manage the operation and administration of the plan. The named fiduciary is identified in the plan document or pursuant to a procedure specified in the plan. See 29 U.S.C. § 1102. A person who is not serving as a named fiduciary may nonetheless be a fiduciary with respect to a particular function they perform.

[18]See 29 U.S.C. § 1104.

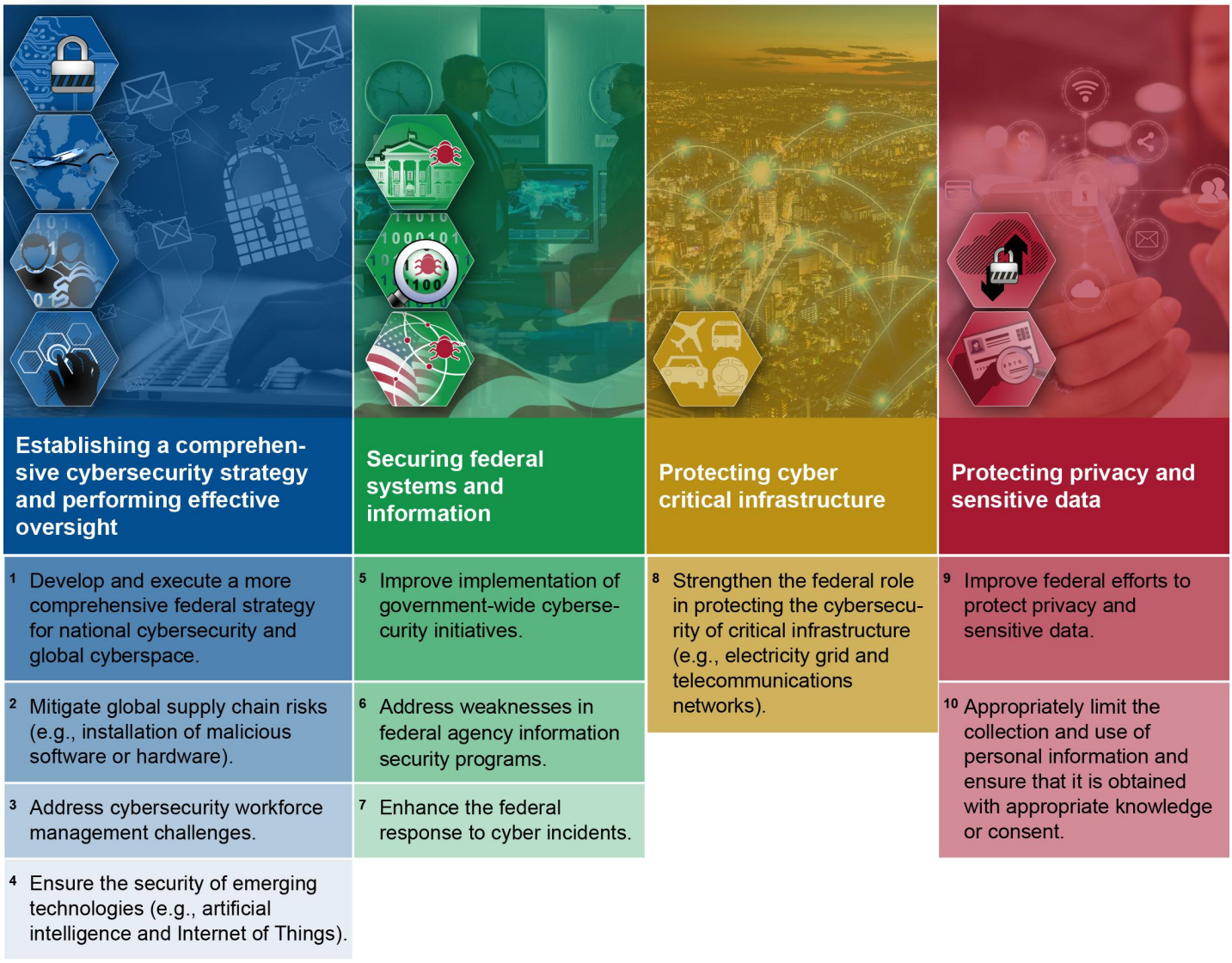
[19]The term "critical infrastructure" as defined in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), refers to systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters. See Pub. L. No. 107-56, § 1016(e), 115 Stat. 272, 401-02 (codified at 42 U.S.C. § 5195c(e)). Federal policy identifies 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

addition, they must effectively respond to data breaches and security incidents when they occur. The risks to systems underpinning the nation's critical infrastructure are increasing, including insider threats from witting and unwitting employees, as security threats evolve and become more sophisticated.

Safeguarding federal IT systems and the systems that support critical infrastructures has been a long-standing concern of GAO. We have designated cybersecurity as a government-wide high-risk area since 1997. We expanded this high-risk area in 2003 to include protection of critical cyber infrastructure and, in 2015, to include protecting the privacy of PII. More recently, in our September 2018 update to our high-risk series, we identified four major cybersecurity challenges that the federal government and other entities face: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data.[20] To address these challenges, we have identified 10 critical actions that the federal government and other entities need to take (see figure 2).

[20]GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sep. 6, 2018).

Figure 2: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges



Source: GAO analysis; images: peshkov/stock.adobe.com; Gorodenkoff/stock.adobe.com; metamorworks/stock.adobe.com; Monster Ztudio/stock.adobe.com. | GAO-21-25

The federal government has been challenged in protecting privacy and sensitive data. Advances in technology have made it easy to correlate information about individuals across large and numerous databases. Further, ubiquitous internet connectivity has facilitated sophisticated tracking of individuals and their activities through mobile devices.

Given that access to data is so pervasive, personal privacy hinges on ensuring that databases of PII maintained by government agencies or on their behalf are protected both from inappropriate access (i.e., data breaches) as well as inappropriate use (i.e., for purposes not originally specified when the information was collected). Likewise, the trend in the private sector of collecting extensive and detailed information about individuals needs appropriate limits. The vast number of individuals potentially affected by data breaches at federal agencies and private sector entities in recent years increases concerns that PII is not being properly protected.[21]

Substantial Sharing of PII and Plan Asset Data Presents Significant Cybersecurity Risks for Defined Contribution Plans

Plan Sponsors and Service Providers Collect and Exchange Extensive Amounts of PII and Plan Asset Data

Selected plan sponsors and service providers—record keepers, TPAs, payroll providers, and custodians—reported sharing a vast amount of PII and plan asset data to assist them in their respective roles in administering DC plans. This is significant in that, according to DOL, in 2018, 106 million plan participants were enrolled in DC plans that held approximately $6.3 trillion in assets.[22] Plan sponsors collect a large amount of PII to enroll participants in a DC plan and then share these data with their service providers to assist them in administering the plan, such as managing account contributions and withdrawals, designing plan documents and benefit statements, handling payroll, and holding plan assets in a bank. The types of participant and beneficiary PII and plan asset data that service providers receive depends on their contractual relationship with the plan sponsor.

[21]GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019).

[22]U.S. Department of Labor, Employee Benefits Security Administration, *Private Pension Plan Bulletin Historical Tables and Graphs 1975-2018* (Washington, D.C.: Forthcoming).

Data collected to enroll participants into and administer DC plans include, but are not limited to, the following:[23]

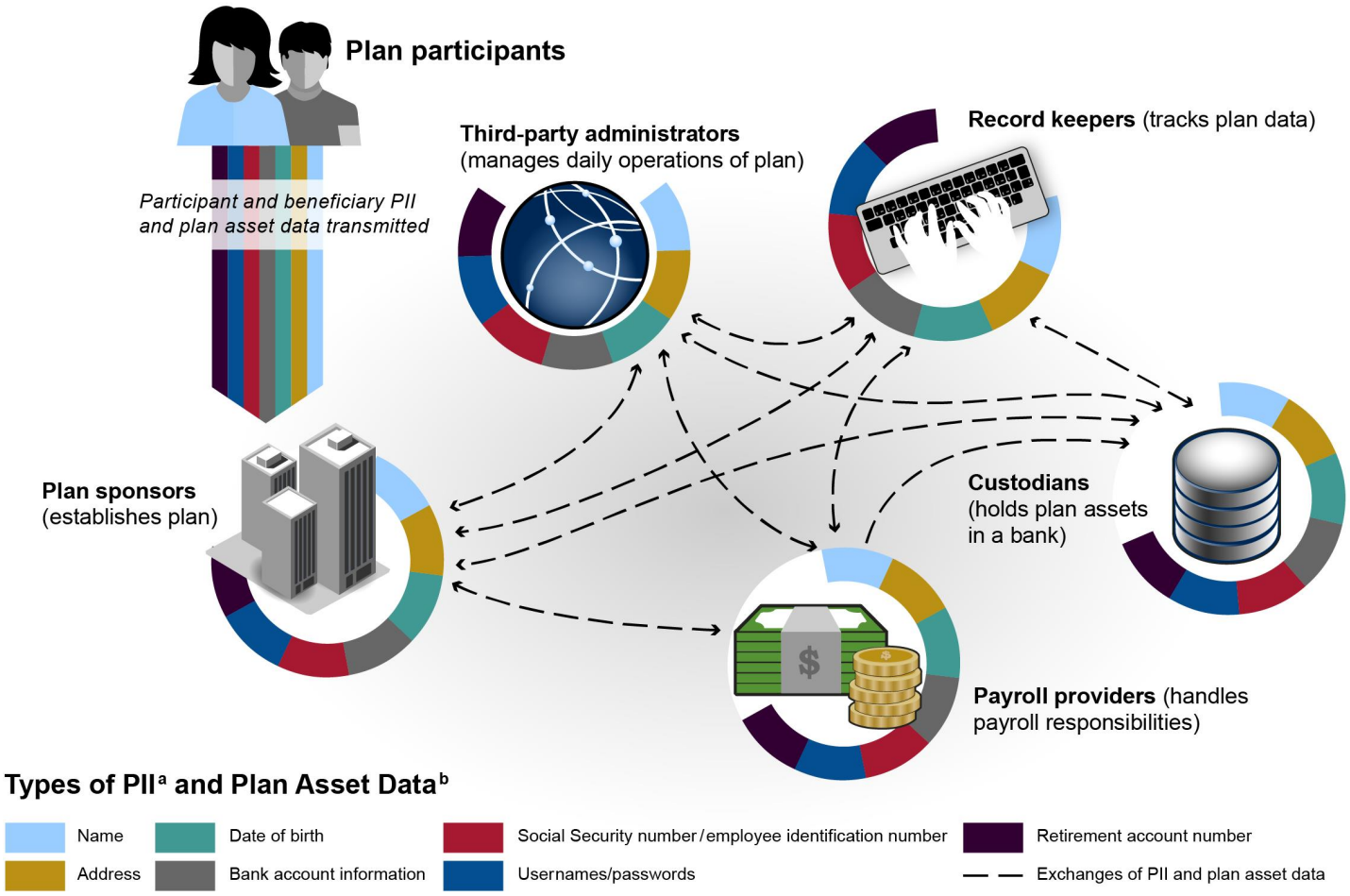
- Participant and beneficiary PII: Name, Social Security number, date of birth, address, username, and password;
- Participant and beneficiary plan asset data: Retirement account number and bank account information.

Once collected, plan sponsors and their service providers store these sensitive data in their information systems and exchange the data with one another in order to deliver essential services to the plan and participants. Ten out of 11 service providers reported receiving all elements of PII and plan asset data mentioned above from the plan sponsors to execute their specific responsibilities, with the exception of a custodian that reported not receiving usernames and passwords.[24] Further, seven service providers reported exchanging PII and plan asset data with each of the other service providers, with the exception of one record keeper that reported being unsure if it exchanged information with custodians, one TPA that reported it does not exchange information with custodians, and two custodians that reported they did not need to exchange information with payroll providers to fulfill their responsibilities to the plan. Figure 3 depicts the collection and sharing of PII and plan asset data among these entities involved in administering DC plans.

[23]For reporting purposes, we included a subset of PII and plan asset data that are collected and shared by plan sponsors and service providers; these pieces of information are key to being able to fraudulently access a retirement account. Other data are collected and shared, such as data on account balances, investment data, and employment information.

[24]We discussed what PII and plan asset data plan sponsors and service providers exchange during the administration of private sector DC retirement plans in the United States with representatives from 13 key entities – two plan sponsors and 11 service providers, including two custodians, one payroll provider, two plan sponsors, five record keepers, and three TPAs.

Figure 3: Personally Identifiable Information (PII) and Plan Asset Data Sharing Among Plan Sponsors and Service Providers in the Administration of Defined Contribution Plans



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

[a]PII 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. For reporting purposes, we included only a subset of PII that is collected and shared by plan sponsors and service providers to administer DC plans. Other data are collected and shared, such as data on account balances, investment data, and employment information.

[b]For reporting purposes, we have defined "plan asset data" as sensitive information that is associated with participants' retirement assets, such as their retirement account number and bank account information.

Plan sponsors and service providers reported using various methods to exchange participant and beneficiary PII and plan asset data. Specifically, all 13 entities reported using an online portal or another electronic

method, such as email or secure file transfer protocol,[25] to exchange information.[26] Further, one plan sponsor and six service providers that reported using electronic methods to exchange data also reported receiving PII and plan asset data via postal mail and/or fax machine.

Protecting PII and plan asset data is critical because the loss or unauthorized disclosure of this sensitive information can lead to serious consequences, such as identity theft or theft of retirement savings. While some identity theft victims can resolve their problems quickly, others face substantial costs, inconvenience, and distress in repairing damage to their credit records.

Collection and Exchange of Participants' PII and Plan Asset Data Present Significant Cybersecurity Risks for DC Plans

Cyber threats directed at plan sponsors and their service providers, as well as plan participants and their beneficiaries, may vary in terms of technical sophistication and financial impact. The threats can include targeted and untargeted attacks that may adversely affect computers, software, a network, a company, or the internet itself. The potential impact of these threats is amplified by the connectivity among information systems, the internet, and other infrastructure used for administering DC plans. Some actors that can cause threats to IT systems (referred to as "threat actors") only seek to steal participants' PII, while others aim to steal assets from an account. According to the 2019 Official Annual Cybercrime Report, cyber attacks are the fastest growing crime in the United States with a global cost in excess of $6 trillion annually by 2021, up from $3 trillion in 2015.[27] Table 1 describes common types of cyber threats that plan sponsors, service providers, participants, and beneficiaries can face during the administration of DC plans.

[25]Secure file transfer protocol provides organizations with a higher level of file transfer protection through the use of encryption to keep data unreadable while in transit to a third party.

[26]We discussed what PII and plan asset data plan sponsors and service providers exchange during the administration of private sector DC retirement plans in the United States with representatives from 13 key entities—two custodians, one payroll provider, two plan sponsors, five record keepers, and three TPAs.

[27]Cybersecurity Ventures, *2019 Official Annual Cybercrime Report* (Northport, NY: Dec. 7, 2018).

Table 1: Common Types of Cyber Threats and Vulnerabilities Relevant to Defined Contribution Plans

Cyber threats /vulnerabilities	Description
Malware	Malware, short for malicious software, is a blanket term for all viruses, worms, Trojans, spyware, and other harmful computer programs used by threat actors to cause destruction and gain access to sensitive information. For example, a threat actor could use spyware, which collects information about users' activities without their knowledge or consent, to gather sensitive data.
Ransomware	Ransomware is malicious software used to deny access to information technology systems or data—to hold systems or data hostage until a ransom is paid. For example, an employee receives an email that looks legitimate—but with one click on a link, or one download of an attachment, everyone is locked out of the company's network until the company pays a ransom to the threat actor.
Phishing	Phishing involves threat actors sending an email designed to trick an individual into divulging PII, such as passwords, plan asset data or bank account information, which can lead to a compromised account. For example, an individual may receive an email that looks like a legitimate customer request from their retirement plan, asking them to click a link, or give their password or other sensitive information, which could offer an attacker access to the individual's account and facilitate theft of retirement funds.
Spoofing	Spoofing involves threat actors creating a fraudulent website to mimic an actual, well-known website run by another party. E-mail spoofing occurs when the sender address and other parts of an email header are altered to appear as though the email originated from a different, more legitimate source.
Business email compromise	Business email compromise scams attempt to deceive organizations into sending money or employees' PII to a threat actor or to use the organization's name to fraudulently obtain material goods. For example, a threat actor poses as an employee or senior official and requests the finance department to send a wire transfer.
Social engineering	Social engineering is a manipulation technique used by cybercriminals to trick people into giving up confidential information. Social engineering relies on the basic human instinct of trust to steal personal and corporate information that can be used to commit further cybercrimes. For example, cybercriminals are using Coronavirus Disease 2019 as a social engineering theme in email, text message, phone, and in-person attacks.
Account takeover	Account takeover occurs when a threat actor fraudulently transfers assets out of an account, such as a retirement plan account. After gaining access to the account, the threat actor collects information that can be used repeatedly to initiate fraudulent transactions. For example, a threat actor might gain access to a retirement account online and divert funds to their own bank account.
Data exfiltration	Data exfiltration is a technique used by a threat actor to target, copy, and transfer sensitive data. For instance, the threat actor can use the forwarding rule in Microsoft Outlook to receive copies of emails that the target user receives. The threat actor can then draft a targeted email to use in carrying out an attack, or, in some cases, to obtain confidential documents.
Privilege abuse	Privilege abuse is a type of threat in which an insider uses legitimate access to systems and data to perform malicious activities. For example, employees can use their privileged accounts to access internal systems and steal sensitive data or assets without being noticed.
Reliance on third-party vendors	Reliance on third-party vendors can present risks to a company when it relies on them to support its business operations, such as payroll and other financial services. This may require the third party—such as a retirement plan record keeper—to access the company's data and its internal information and IT systems. In some instances, the third-party vendor may collect and store the company's data onto its own systems, which may lead to an increased risk of attacks.

Source: GAO analysis of government and private sector information security publications. | GAO-21-25

Note: This list is not meant to be an exhaustive list of all possible cyber threats/vulnerabilities.

A variety of threat actors pose significant cybersecurity risks to DC plans and many of them are becoming increasingly adept at carrying out

attacks. According to the 2019 Worldwide Threat Assessment of the U.S. Intelligence Community, financially motivated threat actors will likely expand their targets in the United States in the next few years.[28] Table 2 lists common types of threat actors that the U.S. intelligence community and other sources have identified.

Table 2: Common Cyber Threat Actors Capable of Attacking Defined Contribution Plans

Threat actor	Description
Criminal groups	Seek to use cyber attacks for monetary gain. Organized criminal groups, which may include organized crime organizations, use spam, phishing, and spyware/malware to commit identity theft, online fraud, and computer extortion.
Hackers	Break into networks for a challenge, revenge, stalking, or monetary gain, among other reasons. Hackers no longer need a great amount of skill to compromise IT systems because they can download commonly available attack tools.
Insiders	Possess authorized access to an information system or enterprise. Insiders may not need a great deal of knowledge of information technology because their position often enables them to gain unrestricted access to cause damage to the system or to steal system data.

Source: GAO analysis of government and private sector information cybersecurity publications. | GAO-21-25

Note: This list is not meant to be an exhaustive list of all possible threat actors.

Cyber Attacks Reported within Defined Contribution Plans in the United States

Current sources of information on cyber attacks do not break down the numbers by industry, including those specific to DC plans; however, in recent years, a number of legal claims allege that unauthorized access to and distribution of retirement plan assets have occurred, resulting in a loss in retirement plan assets which, to date, have not been fully recovered. For example, a plan participant filed a claim that alleged that between December 2018 and January 2019, a threat actor was able to obtain $245,000 from an unauthorized distribution of a participant's retirement account after the threat actor had obtained some of the participant's PII, including the last four digits of their Social Security number and date of birth, and gained access to the participants online retirement account. In addition, another claim was filed that alleged that

[28]Daniel R. Coats, Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community*, testimony before the Senate Select Committee on Intelligence, 116th Cong. 1st session, January 29, 2019.

sometime after December 2015, threat actors were able to obtain more than $400,000 from the participant's retirement account by submitting fraudulent forms to a plan administrator that appeared to be from the participant's work email account.

While the cases mentioned above are currently underway, others have been resolved or settled including two involving inside threat actors employed by plan sponsors. For example, the parties settled a case involving a participant who filed a claim involving multiple entities responsible for the administration of their retirement plan alleging that between September and October 2016, threat actors obtained $99,000 in three separate unauthorized distributions from their retirement account. In another case, the owner of a company gained unauthorized access to four employee's accounts and stole more than $40,000 collectively from their accounts after the company shut down in June 2010. In a different case, another investigation determined that an inside threat actor from a plan sponsor organization failed to remit employee contributions in the amount of $31,882 to its company's plan. In two of these cases, the threat actors were ordered to return the plan assets.

DOL Has Not Provided Guidance to Mitigate Cybersecurity Risks

Existing Guidance Could Help Mitigate Cybersecurity Risks in Defined Contribution Plans

Federal Mitigation Efforts

Several federal reporting requirements, guidance, and tools exist to help mitigate cybersecurity risks for DC plan sponsors and service providers. The plan sponsors and service providers included in this report may be considered financial institutions for regulatory purposes and would be subject to relevant federal cybersecurity requirements or standards. For example, custodians hold plan assets in their bank and payroll providers handle plan sponsors' payroll responsibilities, each of which could be considered financial activities.

Federal reporting requirements and rules include the following:

- Gramm-Leach Bliley Act (GLBA). This act was enacted in 1999 to expand and tighten consumer data privacy safeguards and

restrictions among financial institutions.[29] Under GLBA, a financial institution is defined as any institution that engages in financial activities and has "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[30] The act required certain federal agencies to establish standards for administrative, technical, and physical safeguards that financial institutions must follow.

- Federal Trade Commission Safeguards Rule. This rule implements the security requirements of the GLBA, and requires financial institutions under the FTC's jurisdiction to have measures in place to keep customer information secure.[31] To comply with the rule, FTC has stated that financial institutions must develop and document an information security program that, among other things, must identify and assess the risks to customer information, design and implement information safeguards to control risks, and select service providers that can maintain appropriate safeguards.[32]

However, the GLBA requirements and the FTC Safeguard Rule may not be applicable to all of the parties involved in administering DC plans, specifically the ones that may not be considered financial institutions. For example, the requirements may not apply to plan sponsors whose business may not meet GLBA's definition of engaging in financial activities or other retirement entities that mostly handle administrative duties—such as establishing the plan, tracking participant data and designing plan benefit statements—for the plan sponsor. These entities

[29]See Pub. L. No. 106-102, 113 Stat. 1338 (codified in relevant part primarily at 15 U.S.C. §§ 6801-6809 and 6821-6827).

[30]See 15 U.S.C. § 6801(a). Subtitle A defines nonpublic personal information as personally identifiable financial information that an institution obtains under any of the following three sets of circumstances: (1) the consumer provides the information to the institution to obtain a financial product or service; (2) the information is about the consumer and results from any transaction involving a financial product or service between the institution and the consumer; or (3) the information is about the consumer and is otherwise obtained in connection with providing a financial product or service to that consumer. Nonpublic personal information also includes lists or groupings of consumers derived from nonpublic personally identifiable information.

[31]See 16 C.F.R. pt. 314.

[32]Financial Institutions and Customer Information: Complying with the Safeguards Rule, available at https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (last accessed on October 14, 2020). FTC's compliance guidance states that the Safeguards Rule covers not only traditional financial institutions, but also entities, regardless of size, that are "significantly engaged" in providing financial products or services.

are potentially left without clear federal requirements or standards to follow to mitigate cybersecurity risks.

Additionally, guidance and tools offered by the federal government to mitigate cybersecurity risks may be helpful for the plan sponsors and service providers; however, the guidance and tools are generally voluntary and therefore do not ensure that these entities are taking appropriate actions to mitigate their cybersecurity risks. In addition, the guidance and tools may not be relevant to all entities involved in the administration of DC plans; therefore a comprehensive set of requirements or standards does not exist for protecting the PII and plan asset data in those plans. Relevant efforts are described below.

- National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity. In 2013, recognizing the importance of addressing cybersecurity risks in the private sector, the President issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity,[33] which called for the Director of the National Institute of Standards and Technology (NIST) to lead the development of a voluntary, risk-based cybersecurity framework that would comprise a set of industry standards and best practices to help organizations manage cybersecurity risks.

In response, NIST, in collaboration with the private sector, academia, and government entities, issued the NIST Framework for Improving Critical Infrastructure Cybersecurity[34] that outlines a flexible approach to mitigating cybersecurity risks and guides organizations—regardless of size, degree of cybersecurity risks, or cybersecurity sophistication—in identifying and prioritizing the actions that are appropriate for their objectives, resources, and risks. The framework includes a recommended set of activities that should be addressed to manage cybersecurity risk, which includes governance, risk assessment, supply chain risk management, access control, security training, and continuous monitoring.

[33]Exec. Order No. 13636, 78 Fed Reg. 11,739 (Feb. 19, 2013).

[34]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, Md.: Feb. 12, 2014). The framework was updated in April 2018. See National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1 (Gaithersburg, Md.: April 2018).

- Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). The agency offers a range of cybersecurity assessments and tools to private sector companies that allow them to evaluate their operational resilience and cybersecurity practices. These assessments and tools include penetration testing,[35] vulnerability scanning and assessments,[36] external dependencies management assessments,[37] phishing campaign assessments,[38] and patch management analysis.[39] In addition, CISA also provides real-time cyber threat, incident, and vulnerability information to the private sector. Five of the 13 retirement entities[40] and attendees of the SPARK discussion group stated they found CISA's efforts to be helpful in mitigating cybersecurity risks and used the information on threats and vulnerabilities to create risk awareness and mitigation strategies within their companies.
- Cybersecurity Resources for Small Businesses. Nineteen out of 29 industry stakeholders we spoke to agreed that smaller plan sponsors and service providers face unique challenges in mitigating cybersecurity risks and could benefit from additional educational resources.[41] Some federal resources are dedicated to assist small businesses with cybersecurity risk management. For example, FTC

[35]Penetration testing simulates the tactics and techniques of threat actors to identify and validate exploitable pathways.

[36]Vulnerability scanning and assessments are designed to identify vulnerabilities that threat actors could potentially exploit to compromise network security controls.

[37]External dependencies management assessments are used to evaluate the external dependency management cybersecurity practices of critical infrastructure owners and operators.

[38]Phishing campaign assessments provide an opportunity for determining the potential susceptibility of personnel to phishing attacks.

[39]Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems to correct security and functionality problems in software and firmware.

[40]We analyzed interview responses from the 13 key entities to assist in understanding the extent to which federal efforts assist plan sponsors and service providers in mitigating the cybersecurity risks facing private sector DC retirement plans in the United States.

[41]We discussed cybersecurity resources for small businesses with 29 of the industry stakeholders including officials from seven national organizations representing a range of stakeholders, 11 attorneys and two academics who specialize in ERISA, retirement plans, or cybersecurity, representatives from six insurance companies that offer cyber insurance, and three retirement plan service providers. We only discussed cybersecurity resources for small businesses with the industry stakeholders who had expertise with this subject.

published a website that provides cybersecurity resources for small businesses; this website covers topics such as what first-party cyber insurance plans should cover,[42] how ransomware attacks happen and how to protect against them, and information on how to ensure third-party vendors are securing their systems. In addition, NIST has also developed a website that provides planning guides to help evaluate businesses' current approach to cybersecurity and plan for improvements, links to their cybersecurity guidance and training resources.

Industry Mitigation Efforts

The financial industry and retirement industry have developed several information sharing efforts and leading practices and standards designed to assist companies with mitigating cybersecurity risks. Similar to the guidance and tools described above, these practices and standards are generally voluntary and only apply to certain entities involved in the administration of DC plans, leaving some entities potentially without a comprehensive set of practices or standards to guide them in implementing data protection. Further, the efforts do not provide a standard recommended level of data protection for all of the entities involved in the administration of DC retirement plans. Relevant industry efforts include the following:

- The Society of Professional Asset Managers and Record Keepers Institute Cybersecurity Leading Practices. In September 2017, SPARK[43] developed voluntary standards for how its members should report their cybersecurity capabilities to plan sponsors.[44] According to the Chair of SPARK's Data Security Oversight Board, the intent behind creating the standards was to establish a base of assurance between record keepers and the plans they serve and to communicate how they are protecting the data in their possession. The standards help record keepers communicate and assure the full capabilities of their cybersecurity systems using 16 security control categories, which include, but are not limited to, risk assessment and

[42]Cyber insurance is an industry tool that is available to help plan sponsors and service providers manage cybersecurity risk and recover from cyber attacks.

[43]SPARK is a member-driven, nonprofit organization that helps shape national retirement policy by developing and advancing positons on critical issues that affect plan sponsors, participants, service providers, and investment providers.

[44]The SPARK Institute, Inc., *Industry Best Practice Data Security Reporting, Release 1.0* (Simsbury, Conn.: Sept. 20, 2017).

treatment, security policy, organizational security, access control, compliance, cloud security, and encryption. Each of the five record keeper companies we spoke to reported using the practices and felt they were a helpful tool. They also reported that using the practices has allowed their organization to increase awareness of security issues amongst their employees, which has led to more conversations about security throughout their organization.

- The American Institute of Certified Public Accountants (AICPA) System and Organization Control for Cybersecurity Framework. In 2017, AICPA[45] developed a voluntary tool that assesses an organization's cybersecurity risk management program[46] to help them understand the effectiveness of their security controls. The framework has two different types of assessment tools that an organization can choose from: System and Organization Control (SOC) 1 and SOC2. The SOC1 assessment report contains a general opinion about the effectiveness of controls within the cybersecurity risk management program; it does not include a description or the results of the detailed tests related to system controls relevant to security, availability, processing integrity, confidentiality, or privacy performed by a certified public accountant. The SOC2 assessment is designed to report on controls relevant to the systems at the organization used to process users' data and provides information needed to understand the effectiveness of those controls. Nine of the 13 retirement entities we spoke to reported using the SOC1 or SOC2 to evaluate their cybersecurity programs.[47]
- Financial Services Information Sharing and Analysis Center (FS-ISAC). Established by the financial services sector, FS-ISAC shares threat and vulnerability information, conducts education and training

[45]The AICPA represents the Certified Public Accountant (CPA) profession nationally regarding rule making and standard setting. The AICPA develops standards for audits of private companies and other services by CPAs; provides educational guidance materials to its members, develops and grades the Uniform CPA Examination, and monitors and enforces compliance with the profession's technical and ethical standards.

[46]A cybersecurity risk management program is a set of policies, processes, and controls an entity's management puts into place to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented.

[47]We analyzed interview responses from the 13 key entities to assist in understanding the extent to which industry efforts assist plan sponsors and service providers in mitigating the cybersecurity risks facing private sector DC retirement plans in the United States.

programs, and fosters collaborations with other key sectors and government agencies.[48] In 2018, FS-ISAC, in partnership with SPARK, created the Retirement Industry Council to help promote voluntary information sharing and threat intelligence to members within the retirement industry. According to an article by SPARK, the Retirement Industry Council focuses on the combination of physical and cybersecurity threats faced by the retirement industry and provides trusted leading practices for security controls. Nine of the 13 retirement entities we spoke to stated that they are members of FS-ISAC or the Retirement Industry Council, and that FS-ISAC has been a key resource on cyber threats for the financial sector and has built a high level of trust with its members.

- Cybersecurity Insurance. This type of insurance offers financial benefits that may help plan sponsors and service providers recover from a cyber attack. For example, first-party cyber coverage may pay the insured company's costs following a cyber attack, such as for investigating the attack, restoring the affected IT systems, and notifying people whose PII was compromised. Third-party coverage may pay for losses and costs to external parties, such as for expenses relating to disputes or lawsuits.

However, industry stakeholders told us that cyber insurance also has some limitations.[49] Eleven of 19 stakeholders said that cyber insurance policies generally do not replace funds stolen from participants' accounts and frequently have provisions, such as caps on payouts or exclusions for certain types of attacks, which limit the amount of coverage for a cyber attack. Additionally, 12 of 19 stakeholders stated that plan sponsors may not understand what their cyber policies actually cover, for reasons that include a lack of consistent terminology, policy types, and pricing models across the cyber insurance industry. Five stakeholders added that employers usually purchase cyber insurance for their entire enterprise, which may not be tailored to or adequate for the specific needs of a retirement plan, such as replacing stolen retirement account funds.

[48]FS-ISAC was started in 1999 as a member-owned nonprofit that entered into partnerships with other industry groups, associations, and government agencies. It has broad industry representation, with more than 5,000 members worldwide, and has 30 permanent staff working fulltime on threat analysis and information sharing.

[49]We discussed cyber insurance with 19 industry stakeholders, including representatives from six insurance companies, seven ERISA attorneys, two academics, and four national organizations representing retirement industry stakeholders.

DOL Has Not Formally Stated Whether Cybersecurity is a Responsibility for Plan Fiduciaries

Under ERISA, DOL is responsible for protecting the rights and financial security of plan participants and for assuring the integrity and effective management of the private pension system in the United States. Within DOL, EBSA's mission is to assure the security of the retirement benefits of U.S. workers and their families. One way the agency accomplishes its mission is by assisting and educating workers, plan sponsors, fiduciaries and service providers on their responsibilities. Of 22 stakeholders we interviewed, 21 expressed the view that a fiduciary's responsibility under ERISA includes mitigating cybersecurity risks in DC plans.[50] DOL officials told us that, in their view, the fiduciary obligations under ERISA apply to managing cybersecurity risks of both retirement plan assets and PII.[51]

Plan fiduciaries potentially assume fiduciary responsibility for hiring service providers who administer the plan, including oversight of providers' cybersecurity postures. For example, DOL officials and several stakeholders, including two ERISA attorneys and representatives from a national retirement organization representing sponsors of mutual funds used in retirement plans, said that a plan fiduciary's responsibility to mitigate cybersecurity risks would extend to overseeing any entity providing services to retirement plans. DOL guidance describes the hiring of a service provider as a fiduciary function,[52] and DOL officials told us that this includes asking service providers questions about their cybersecurity. The guidance also describes how a plan sponsor can set

[50]We discussed fiduciary responsibility to mitigate cybersecurity risk in retirement plans with DOL officials and 21 other stakeholders, including representatives from national organizations comprised of retirement industry stakeholders, ERISA attorneys, service provider representatives, and an academic.

[51]DOL regulations related to plan disclosure and record retention through the use of electronic media require plan administrators and record keepers to take reasonable steps to ensure that participant information is protected and secured. See 29 C.F.R. §§ 2520.104b-1(c), 2520.104b-31, and 2520.107-1.

[52]The guidance further states that for a service contract or arrangement to be reasonable, service providers must provide certain information to the fiduciary about the services they will provide to the plan and all of the compensation they will receive. The guidance also lists additional items a fiduciary needs to consider when selecting a service provider, including: information about the firm itself; information about the quality of the firm's services; and a description of the firm's business practices including whether the firm has fiduciary liability insurance. See U.S. Department of Labor, *Meeting Your Fiduciary Responsibilities* (Washington, D.C.: Sept. 2017).

up agreements with service providers they hire so that the provider assumes fiduciary liability for certain functions.[53] Three ERISA attorneys and representatives from a national retirement organization representing plan sponsors and service providers told us that service providers can be a source of elevated cybersecurity risk for fiduciaries because they handle PII and plan asset data; six ERISA attorneys told us that plan fiduciaries may remain responsible for the actions of their service providers under ERISA.

Although a compelling need exists, DOL has not issued a formal statement, either in a document or on its website, on whether it is a fiduciary's responsibility to mitigate cybersecurity risks in retirement plans, according to DOL officials.[54] Reflecting their acknowledgement of cybersecurity risk mitigation as a fiduciary function, DOL officials told us that the agency has begun an initiative to provide public-facing guidance to fiduciaries and service providers on securing their IT systems. DOL officials told us that they were uncertain when they would release the guidance to the public and were unable to provide details on the content of the guidance or an assurance that the guidance would clear the agency's internal review process. DOL officials said that they believe cybersecurity is a large problem for retirement plans,[55] and that the agency has conducted investigations and prosecutions related to cybersecurity incidents, both civil and criminal.[56] DOL officials also

[53]For example, if an employer appoints an investment manager that is a bank, insurance company, or registered investment adviser, the employer is responsible for the selection of the manager, but is not liable for the individual investment decisions of that manager, according to DOL's guidance. However, an employer is required to monitor the manager periodically to assure that it is handling the plan's investments prudently and in accordance with the appointment.

[54]DOL has primary responsibility for administering and enforcing the fiduciary responsibility provisions under Part 4 of Title I of ERISA.

[55]A range of stakeholders, including ERISA attorneys and representatives from national retirement organizations, pointed to several ongoing court cases that alleged participant asset losses and unauthorized disclosure of participant PII in retirement plans; however, four ERISA attorneys and a representative from a retirement plan service provider said that the federal courts have not ruled on the question of whether managing cybersecurity risks is a fiduciary function.

[56]DOL officials told us that complaints come from participants, service providers, state regulators, and law enforcement offices such as the Office of the Inspector General, and the Federal Bureau of Investigation. Cases involve both plan sponsors and service providers, specifically TPAs and record keepers, and include issues such as unauthorized distributions from accounts. DOL officials also provided examples of their involvement in several public criminal cases involving identify theft and other cyber attacks.

explained that by design, ERISA is meant to be broad and apply to a wide range of activity, and that its general fiduciary obligations of prudence and loyalty include cybersecurity as well as any other part of plan administration.[57] DOL officials told us that they expect plan administrators to keep their IT systems secure as part of their fiduciary responsibility.

Nevertheless, without formal clarification from DOL, fiduciaries could face legal challenges if they fail to meet their responsibilities to protect retirement benefits, plan assets, and participant PII. For example, five ERISA attorneys stated that they believe that a fiduciary's failure to mitigate cybersecurity risk could lead to possible legal liability. One of these attorneys said that plan fiduciaries who fail to mitigate cybersecurity risks in retirement plans may be exposed to litigation if plan assets or PII are compromised by a cyber attack. An ERISA attorney who is also an academic in the employee benefits field said that fiduciaries who do not use sufficient preventative measures to protect plan assets and PII may be found to have violated their fiduciary duties. Another ERISA attorney told us that litigation will likely lead courts to decide where responsibility lies for participant losses stemming from a cyber attack; he added that he thought that courts would determine liability for losses based on which party could have prevented the attack. For example, if an attack occurred in a record keeper's systems that lacked adequate safeguards, the record keeper could be responsible, according to this attorney. On its website, DOL states that fiduciaries who do not follow ERISA's principles of conduct[58] for fiduciaries may be personally liable to restore any losses to the plan.[59] DOL officials added that there is a risk that some fiduciaries may not be able to cover losses because of the large amount of money potentially at risk in retirement accounts.

Without DOL formally stating whether mitigating cybersecurity risks is a plan fiduciary's responsibility, retirement plan administrators may find it difficult to understand what is expected of them with respect to mitigating cybersecurity risks. Further, plan participants cannot be assured that plan

[57]DOL officials also pointed out that many activities similarly covered under the duty of prudence and loyalty do not have specific regulations associated with them but are required nonetheless.

[58]The principles of conduct referred to on DOL's website are the fiduciary duties described in 29 U.S.C. § 1104.

[59]See https://www.dol.gov/general/topic/retirement/fiduciaryresp; accessed on September 1, 2020.

administrators are adequately securing their PII and plan asset data to minimize identity theft and potential losses of their retirement assets.

DOL Has Not Provided Guidance That Identifies Minimum Expectations for Cybersecurity Risk Mitigation to Plan Sponsors and Service Providers

In 2011 and 2016, the ERISA Advisory Council[60] released two reports to DOL that focused on privacy and cybersecurity issues affecting employee benefit plans, which included DC plans. The reports emphasized the need for plan sponsors and service providers to protect the data they use to administer retirement plans.

- The 2011 report pointed out that ERISA does not directly address whether and how employee retirement plans should protect PII of participants and beneficiaries of retirement benefit plans.[61] More specifically, the report suggested DOL develop materials that highlight the need for plan sponsors to address privacy and security in plan administration, and outline factors to consider and adopt when developing and implementing privacy and security policies and highlight methods available for monitoring actions plan administrators take with respect to privacy and security.
- Expanding on the previous report, the 2016 report focused on information that would be useful to plan sponsors, fiduciaries, and their service providers in evaluating and developing a cybersecurity program for their retirement plans.[62] The report pointed out that plan sponsors and fiduciaries may be challenged by the lack of clear standards surrounding cybersecurity and recommended that DOL

[60]The Advisory Council on Employee Welfare and Pension Benefit Plans, usually referred to as the ERISA Advisory Council, was established under Section 512 of ERISA to advise the Secretary of Labor on matters related to welfare and pension benefit plans. The council consists of 15 members appointed by the Secretary of Labor, which includes representatives from employee organizations, employers, the general public, and the fields of insurance, corporate trust, actuarial counseling, investment counseling, investment management, and accounting.

[61]Advisory Council on Employee Welfare and Pension Benefit Plans, *Report to the Honorable Hilda L. Solis, United States Secretary of Labor, Privacy and Security Issues Affecting Employee Benefit Plans* (Washington, D.C.: Nov. 9, 2011).

[62]Advisory Council on Employee Welfare and Pension Benefit Plans, *Report to the Honorable Thomas E. Perez, United States Secretary of Labor, Cybersecurity Considerations for Benefit Plans* (Washington, D.C.: November 2016).

provide information to plan fiduciaries to educate them on cybersecurity risks and potential approaches for managing these risks. The report described several cybersecurity frameworks that have been developed to help organizations evaluate and navigate cybersecurity risks, including NIST's framework, which could provide the foundation for cybersecurity strategies for benefit plans.

EBSA officials stated that the reports were released to the public through their website but had not taken or planned to take any action on the recommendations in the reports.

Twenty-four of 34 industry stakeholders[63] we spoke with said they were not aware of any comprehensive federal regulations or guidance governing cybersecurity standards for retirement plans and 10 retirement entities and attendees of the SPARK discussion group stated that the industry could benefit from DOL providing guidance in this area. For example, an academic in the employee benefits field stated that DOL has not done very much to assist plan fiduciaries and participants with mitigating cybersecurity risks. He stated that there is a need for DOL to take actions on issues highlighted in the ERISA Advisory Council reports on cybersecurity, particularly with respect to providing leading practices to mitigate cybersecurity risks. In addition, an ERISA attorney stated that in her view DOL needs to provide further details about what fiduciaries need to do regarding cybersecurity, particularly related to specific information security control expectations and cybersecurity risk management practices[64], in order to fulfill its duties. Lastly, representatives from a custodian company stated that they would like to see federal guidelines and regulations outlining specific cybersecurity responsibilities, including standards or leading practices for retirement plan entities.

[63]To assist in understanding the extent to which federal efforts exist to require or assist plan sponsors and service providers in mitigating the cybersecurity risks facing private sector DC retirement plans in the United States, we spoke to 34 industry stakeholders including (1) 10 national organizations representing retirement industry stakeholders; (2) the ERISA Advisory Council; (3) 11 attorneys and two academics who specialize in ERISA, retirement plans, or cybersecurity; (4) a financial sector group that specializes in sharing threat information; (5) representatives from six insurance companies that offer cyber insurance; and (6) three retirement plan service providers. We only discussed the issue with the industry stakeholders who had expertise with this subject.

[64]Cybersecurity risk management comprises a full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats; maintain awareness of cyber threats; detect anomalies and incidents adversely affecting IT and data; and mitigate the impact of, respond to, and recover from incidents.

While DOL has issued regulations on e-disclosures that require plan administrators to take appropriate and reasonable measures to ensure the protection of confidential participant information,[65] it has not identified minimum cybersecurity expectations for plan sponsors and service providers. Specifically, the regulations do not specify how plan sponsors and service providers are to meet these security requirements or what expectations should be used to evaluate and confirm that the protections are sufficient.

DOL officials stated that, in their view, cybersecurity was a serious problem for retirement plans and that they intend to issue public-facing guidance that would address several cybersecurity-related issues. However, they could not describe the specific contents of the guidance nor were they certain when it will be issued.

As DOL considers guidance on cybersecurity-related issues, it could adopt existing cybersecurity standards, such as NIST's framework, the other frameworks outlined in the 2016 ERISA Council Report,[66] or the standards used to safeguard data and PII in the financial sector. Alternatively, DOL could consider convening a group comprised of relevant stakeholders and experts to come up with an agreed-upon set of cybersecurity standards for ERISA plans.

Without guidance identifying expectations for the protection of PII and plan asset data, DOL cannot be assured that this sensitive information is being adequately or consistently protected. Further, the gaps and inconsistencies in how plan sponsors and their service providers implement appropriate security measures will continue to exist. This potential lack of adequate and consistent protection could result in substantial harm to participants and beneficiaries including loss or theft of money, identity theft, or litigation of plan fiduciaries and their administrators.

[65]See 29 C.F.R. §§ 2520.104b-1(c) and 2520.104b-31. In promulgating its recent safe harbor for using electronic media to furnish participant disclosure under 29 C.F.R. § 2520.104b-31, DOL stated its view that, as required by ERISA, it expects that many plan administrators, or their service or investment providers, already have secure systems in place to protect covered individuals' personal information. See 85 Fed. Reg. 31,884, 31,916 (May 27, 2020).

[66]The other frameworks outlined in the 2016 ERISA Advisory Council report are: the *Support Anti-Terrorism By Fostering Effective Technologies Act of 2002* ("SAFETY Act"); *SPARK Best Practices*; *Health Information Trust Alliance* ("HITRUST"); and *the AICPA Initiatives and SOC Reporting*.

Conclusions

Private sector employer-sponsored DC retirement plans are a crucial component of retirement security for millions of Americans. In many cases, they may hold a participant's life savings. A single cyber attack at any point in the complex web of entities working together to administer a retirement plan could cause enormous losses of both PII and plan assets, which could lead to identity theft or severe financial and other ramifications for plan participants. Accordingly, it has become imperative that industry and government prevention and mitigation efforts evolve to keep pace with these threats.

While federal and private sector industry partners have efforts to help mitigate cybersecurity risks, many of these efforts do not directly apply to several of the various entities that administer DC plans. As a result, plan fiduciaries and their service providers rely on a patchwork of federal regulations, guidance, and industry leading practices to help them mitigate cybersecurity risk in DC plans. If DOL is to have reasonable assurance that plans have effective cybersecurity measures in place, it must be sure that plan fiduciaries understand their responsibilities in protecting PII and plan assets. Until DOL formally clarifies plan fiduciaries' responsibilities and provides minimum expectations related to cybersecurity, fiduciaries may not realize that they could be liable for losses they were obligated to prevent, and plans and their participants will continue to be vulnerable to financial losses and PII breaches. Such risks could lead to the erosion of confidence in our nation's private pension system.

Recommendations for Executive Action

We 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)

Agency Comments and Our Evaluation

We provided a draft of this report to Secretaries of the Department of Homeland Security, DOL, and the Department of the Treasury; the chairmen of FTC, the Securities and Exchange Commission, and the Board of Governors of the Federal Reserve System; and the Director of the Pension Benefit Guaranty Corporation for review and comment. In written comments (reprinted in Appendix I), DOL did not indicate whether it agreed or disagreed with our first recommendation and stated that it agreed, with respect to our second recommendation, that increasing cybersecurity awareness would be helpful.

Regarding our first recommendation that DOL formally state whether cybersecurity for private sector employer-sponsored DC retirement plans is a plan fiduciary responsibility under ERISA, DOL stated that plan fiduciaries must act prudently and solely in the interest of plan participants and beneficiaries, as set forth in ERISA section 404. DOL further said that, in its view, these duties require plan fiduciaries to take appropriate precautions to mitigate risks of malfeasance to their plans, whether cyber or otherwise. It also cited existing regulations on electronic records and electronic disclosures that include provisions to ensure systems are safe and personal information is protected. GAO recognizes the importance of these existing regulations for highlighting fiduciary responsibility regarding the cybersecurity of retirement plans. Nevertheless, making a formal statement will help ensure that plan fiduciaries are clear on their responsibility to mitigate cybersecurity risk in private sector employer-sponsored DC retirement plans to better protect PII and plan assets. Without such a formal statement, retirement plan administrators may not be aware of this fiduciary obligation.

Regarding our second recommendation on developing and issuing guidance identifying expectations for mitigating cybersecurity risks, DOL agreed that increasing awareness of fiduciaries' duties under ERISA with respect to cybersecurity would be helpful. DOL stated it is drafting compliance assistance materials to help (1) increase awareness among plan fiduciaries of DOL's position on cybersecurity risk mitigation and (2) ensure that fiduciaries satisfy their ERISA obligations when selecting and monitoring service providers. As noted in our report, we acknowledge DOL's efforts in this area. However, it is also important that DOL identify minimum expectations for mitigating cybersecurity risks for all entities involved in the administration of DC plans. GAO believes that fully implementing this recommendation will provide assurances to the agency,

and to DC plan participants and beneficiaries, that PII and plan asset data are being adequately and consistently protected in DC retirement plans.

We received technical comments from the Department of Homeland Security, DOL, and FTC, which we have incorporated where appropriate. The Board of Governors of the Federal Reserve System, the Pension Benefit Guaranty Corporation, the Securities and Exchange Commission, and the Department of the Treasury also responded indicating they had no written or technical comments.

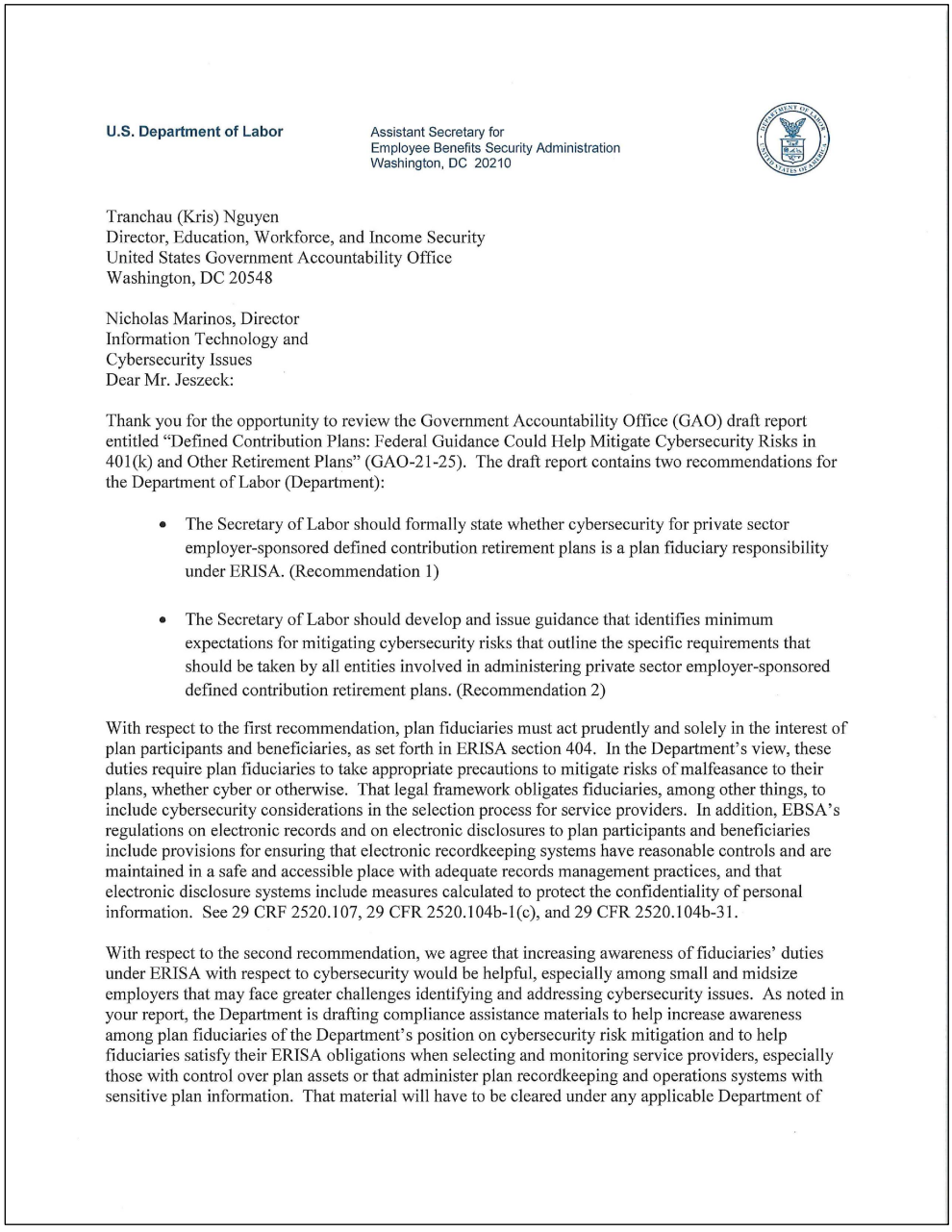
As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the appropriate congressional committees; the Secretaries of the Departments of the Treasury, Labor, and Homeland Security; the Chairmen of the Federal Trade Commission, the Securities and Exchange Commission, and the Board of Governors of the Federal Reserve System, and the Director of the Pension Benefit Guaranty Corporation. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Tranchau (Kris) Nguyen at 202-512-2660 or nguyentt@gao.gov or Nick Marinos at (202) 512-9342 or marinosn@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.

Tranchau (Kris) Nguyen
Director
Education, Workforce, and Income Security

Nick Marinos
Director
Information Technology and Cybersecurity

Appendix I: Comments from the Department of Labor



U.S. Department of Labor

Assistant Secretary for
Employee Benefits Security Administration
Washington, DC 20210

Tranchau (Kris) Nguyen
Director, Education, Workforce, and Income Security
United States Government Accountability Office
Washington, DC 20548

Nicholas Marinos, Director
Information Technology and
Cybersecurity Issues
Dear Mr. Jeszeck:

Thank you for the opportunity to review the Government Accountability Office (GAO) draft report entitled "Defined Contribution Plans: Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans" (GAO-21-25). The draft report contains two recommendations for the Department of Labor (Department):

- 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)

With respect to the first recommendation, plan fiduciaries must act prudently and solely in the interest of plan participants and beneficiaries, as set forth in ERISA section 404. In the Department's view, these duties require plan fiduciaries to take appropriate precautions to mitigate risks of malfeasance to their plans, whether cyber or otherwise. That legal framework obligates fiduciaries, among other things, to include cybersecurity considerations in the selection process for service providers. In addition, EBSA's regulations on electronic records and on electronic disclosures to plan participants and beneficiaries include provisions for ensuring that electronic recordkeeping systems have reasonable controls and are maintained in a safe and accessible place with adequate records management practices, and that electronic disclosure systems include measures calculated to protect the confidentiality of personal information. See 29 CRF 2520.107, 29 CFR 2520.104b-1(c), and 29 CFR 2520.104b-31.

With respect to the second recommendation, we agree that increasing awareness of fiduciaries' duties under ERISA with respect to cybersecurity would be helpful, especially among small and midsize employers that may face greater challenges identifying and addressing cybersecurity issues. As noted in your report, the Department is drafting compliance assistance materials to help increase awareness among plan fiduciaries of the Department's position on cybersecurity risk mitigation and to help fiduciaries satisfy their ERISA obligations when selecting and monitoring service providers, especially those with control over plan assets or that administer plan recordkeeping and operations systems with sensitive plan information. That material will have to be cleared under any applicable Department of

Labor rules and procedures for sub-regulatory guidance before the material can be issued and posted on the Department's website.

Thank you again for the opportunity to review your draft report and recommendations. Please do not hesitate to contact us if you have questions concerning this response or if we can be of further assistance.

Sincerely,

Jeanne Klinefelter Wilson

Jeanne Klinefelter Wilson
Principal Deputy Assistant Secretary

Agency Comment Letter

Text of Appendix I: Comments from the Department of Labor

Page 1

Tranchau (Kris) Nguyen
Director, Education, Workforce, and Income Security
United States Government Accountability Office
Washington, DC 20548

Nicholas Marinos, Director
Information Technology and Cybersecurity Issues

Dear Mr. Jeszeck:

Thank you for the opportunity to review the Government Accountability Office (GAO) draft report entitled "Defined Contribution Plans: Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans" (GAO-21-25). The draft report contains two recommendations for the Department of Labor (Department):

- 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)

With respect to the first recommendation, plan fiduciaries must act prudently and solely in the interest of plan participants and beneficiaries, as set forth in ERISA section 404. In the Department's view, these duties require plan fiduciaries to take appropriate precautions to mitigate risks of malfeasance to their plans, whether cyber or otherwise. That legal framework obligates fiduciaries, among other things, to include cybersecurity considerations in the selection process for service providers. In addition, EBSA's regulations on electronic records and on electronic disclosures to plan participants and beneficiaries include provisions for ensuring that electronic recordkeeping systems have reasonable controls and are maintained in a safe and

accessible place with adequate records management practices, and that electronic disclosure systems include measures calculated to protect the confidentiality of personal information. See 29 CRF 2520.107, 29 CPR 2520.104b-l(c), and 29 CPR 2520.104b-31.

With respect to the second recommendation, we agree that increasing awareness of fiduciaries' duties under ERISA with respect to cybersecurity would be helpful, especially among small and midsize employers that may face greater challenges identifying and addressing cybersecurity issues. As noted in your report, the Department is drafting compliance assistance materials to help increase awareness among plan fiduciaries of the Department's position on cybersecurity risk mitigation and to help fiduciaries satisfy their ERISA obligations when selecting and monitoring service providers, especially those with control over plan assets or that administer plan recordkeeping and operations systems with sensitive plan information. That material will have to be cleared under any applicable Department of Labor rules and procedures for sub-regulatory guidance before the material can be issued and posted on the Department ' s website.

Page 2

Thank you again for the opportunity to review your draft report and recommendations. Please do not hesitate to contact us if you have questions concerning this response or if we can be of further assistance.

Sincerely,

Jeanne Klinefelter Wilson
Principal Deputy Assistant Secretary

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Tranchau (Kris) Nguyen, (202) 512-2660, nguyentt@gao.gov

Nick Marinos, (202) 512-9342, marinosn@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Charles Jeszeck (Director), Marisol Cruz Cain (Assistant Director), Mark Glickman (Assistant Director), David Lehrer (Assistant Director), Ted Burik (Analyst-in-Charge), Shaunyce Wallace (Analyst-in-Charge), Amy Apostol, Christopher Businsky, Nancy Glover, Kirsten Lauber, Catherine Maloney, Brittni Milam, Jessica Moscovitch, Corinna Nicolaou, Jessica Orr, Brian Palmer, Andrew Stavisky, Curtia Taylor, Adam Wendel, and Seyda Wentworth made significant contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Acting Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548