TESTIMONY OF

MIMI BLANCO-BEST

AICPA ASSOCIATE DIRECTOR, ATTESTATION METHODOLOGY AND GUIDANCE

BEFORE THE ERISA ADVISORY COUNCIL ON EMPLOYEE WELFARE AND PENSION BENFIT PLANS

CYBERSECURITY ISSUES AFFECTING HEALTH BENEFIT PLANS

JULY 18, 2022

I am pleased to appear before the Advisory Council on behalf of the American Institute of Certified Public Accountants (AICPA). We commend the Advisory Council for holding this hearing to examine cybersecurity issues affecting health benefit plans including existing relevant frameworks, approaches, and initiatives. My remarks today will focus on the various ways in which CPAs can address clients' cybersecurity efforts. The involvement of a CPA can enable users to place a greater level of trust and confidence in cybersecurity information communicated by those organizations plan sponsors, administrators, employees, and others. Specifically, I will address:

- Cybersecurity risks faced by health benefit plans
- Plan auditor's responsibility for evaluating cybersecurity risk and controls in an audit of a plan's financial statements
- Cybersecurity services CPAs can provide -- *outside the basic financial statements* -- to help plan management assess the effectiveness of a service organization's controls and to communicate such information to users
- Overview of AICPA's System and Organization Control (SOC) Suite of Services and related reporting frameworks, with a focus on how SOC 2 reports and SOC for Cybersecurity reports can provide plan management with information about a service organization's (or other organization's) cybersecurity efforts

Cybersecurity risks faced by health benefit plans

Employee health benefit plans, like pension and retirement plans and other entities, are vulnerable to cyber-attacks and thus exposed to risks relating to privacy, security, and fraud. Health benefit plans may be attractive targets for hackers seeking access to plan assets and participant personal information. Factors that contribute to cyber risk in plans include:

- The electronic environment in which they operate. Electronic benefit plan information is especially susceptible to cyber-attacks because it includes large amounts of sensitive employee information that is shared with multiple third parties, including outsourced service organizations that also maintain and electronically share sensitive employee and asset information.
- Benefit plans often fall outside the scope of a sponsor organization's cybersecurity planning with regard to ongoing business activities.

- Employee benefit plans are not regulated for cybersecurity purposes, as are certain other businesses that handle personal information.
- Plan sponsors and administrators may have a false sense that anti-virus and anti-spam software adequately protect them from these risks.
- Plan sponsors and administrators may have a false sense that a SOC 1 report from their service organizations adequately addresses cyber risks at those organizations.

Plan sponsors, administrators, and service providers maintain electronic information that may be particularly vulnerable to cyber-attacks, including:

- "Personally identifiable information" (PII) such as social security numbers, dates of birth, and email addresses. PII has significant value to cybercriminals because it is permanently associated with an individual (unlike a credit card account number, PII cannot be easily "cancelled") and therefore can be misused over a longer period of time.
- Participant enrollment data, direct deposit information, compensation, and other financial information.
- "Electronic protected health information" (EPHI), which includes information about health status, provision of healthcare, or payment for health care that can be linked to a specific individual, that is produced, saved, transferred, or received in an electronic form.
- Similar to PII, EPHI does not expire, and stolen information can be used to acquire prescription drugs, receive medical care, falsify insurance claims, file fraudulent tax returns, open credit accounts, obtain official government-issued documents such as passports and driver's licenses, and even create new identities.

The consequences of a cybersecurity breach can be substantial for plan sponsors, service providers and participants. Significant costs may be incurred in detecting the extent of the break-in, investigating and managing the incident response, recovering data, and restoring system integrity. The theft of certain PII and breach of online security over plan assets and records can lead to monetary losses to participants, beneficiaries, the plan, the plan sponsor, and service providers. Cybersecurity breaches may result in operational disruption and damage to a sponsor's and administrator's reputation. Plan fiduciaries potentially could be found to be responsible for a fiduciary breach and required to restore losses to the plan participants and beneficiaries. A cybersecurity breach of EPHI in a health plan could result in potential violations of the Health Insurance Portability and Accountability Act (HIPAA) and subject the plan sponsor and service providers to fines or monetary settlements

Plan auditor's responsibility for evaluating cybersecurity risk and controls in an audit of a plan's financial statements

Cybersecurity risks and controls are within the scope of the financial statement auditor's concern only to the extent they could impact financial statements and company assets to a material extent. The Center for Audit Quality (CAQ) discussed the auditor's reporting for cybersecurity in its Alert #2014-03, *Cybersecurity and the External Audit.* The information contained in the Alert is summarized below.

Auditing standards require the financial statement auditor to obtain an understanding of how the company uses IT and the impact of IT on the financial statements. Financial statement auditors also are required to obtain an understanding of the extent of the company's automated controls as they relate to financial reporting, including the IT general controls that are important to the effective operation of

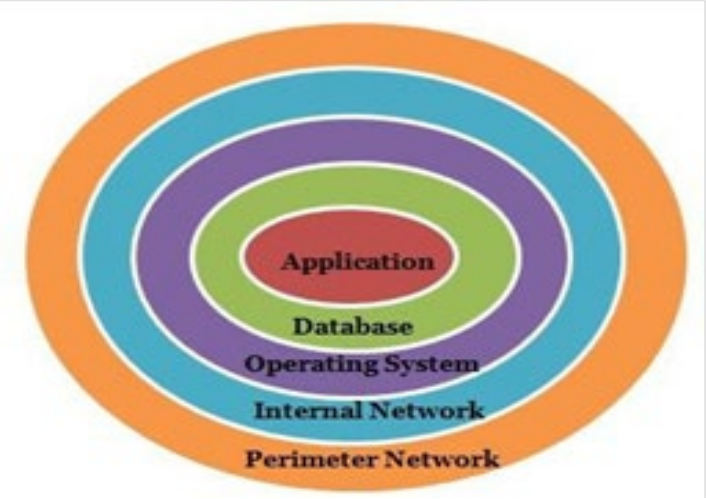
automated controls, and the reliability of data and reports used in the audit that were produced by the company.

In assessing the risks of material misstatement to the financial statements— including IT risks resulting from unauthorized access and unauthorized use or disposition of company assets—financial statement auditors are required to consider their understanding of the company's IT systems and controls. If information about a material breach is identified, the financial statement auditor would need to consider the impact on financial reporting, including disclosures, and the impact on ICFR.

Systems and data in scope for most audits usually are a subset of the totality of systems and data used by companies to support their overall business operations, and the auditor's focus is on access and changes to systems and data that could impact the financial statements and the effectiveness of ICFR. In contrast, a company's overall IT platform includes systems (and related data) that address the operational, compliance and financial reporting needs of the entire organization.

From an operational risk or privacy perspective, companies implement processes and controls to restrict access to their systems, applications, and data, including third party records and other sensitive information. Accordingly, given the focus on a narrower slice of a company's overall IT platform, the execution of an audit of the financial statements in accordance with professional standards likely would not include areas that would address a cybersecurity breach. However, if information about a material breach is identified, the auditor would need to consider the impact on financial reporting, including disclosures, and the impact on ICFR.

The following diagram depicts the typical access path to an IT system:



The auditor's primary focus is on the controls and systems that are in the closest proximity to the application data of interest to the audit—that is, Enterprise Resource Planning (ERP) systems, single purpose applications like a fixed asset system or any set of connected systems that house financial statement related data.

On the other hand, cyber incidents usually first occur through the perimeter and internal network

layers, which tend to be somewhat removed from the application, database, and operating systems that are typically included in access control testing of systems that affect the financial statements. Audit procedures might include testing access controls at the application layer, and at the database and operating system layers, in that order of focus and priority. Other broader elements of security around the perimeter and network layers generally tend not to be within the scope of the financial statement and ICFR audits.

In a plan environment, even when a breach of participant information occurs, it may have no direct effect on the plan's financial statements. This might happen when, for example, participant information was breached but there were no plan assets lost because no participant accounts were accessed. In such situations, the breach would need to be considered, but because there is no effect on financial reporting, the auditor's response may be minimal.

Cybersecurity services CPAs can provide -- outside the basic financial statements -- to help plan management assess the effectiveness of a service organization's controls and to communicate such information to users

For all the reasons previously mentioned, cybersecurity is among the top issues currently on the minds of boards of directors, managers, investors, customers, and other stakeholders of organizations of all sizes, including plan sponsors, administrators, and others. Employee health benefit plans, like other organizations, are under increasing pressure to demonstrate that they are managing cybersecurity threats, and that they have effective processes and controls in place to detect, respond to, mitigate, and recover from breaches and other security events. Managing cybersecurity concerns is especially challenging because even an organization with a highly mature risk management program is susceptible to breaches that may not be detected in a timely manner. Users want timely, useful information about how these organizations are managing cyber threats and about whether their related cybersecurity processes and controls are effective to prevent and detect breaches that could disrupt their business.

To address cybersecurity and other risks, the AICPA developed the System and Organization Controls (SOC) Suite of Services, which include a number of unique service offerings CPAs may provide in connection with system-level controls of a service organization or entity-level controls of all organizations. The SOC suite of services includes the following that may be relevant to employee benefit plans:

- **SOC 1® — SOC for Service Organizations: ICFR.** Service organizations may provide services that are relevant to their user entities' internal control over financial reporting and, therefore, to the audit of financial statements.

- **SOC 2® — SOC for Service Organizations: Trust Services Criteria**. To identify, assess and address the risks that arise from doing business with a service organization, customers and business partners want information about the design, operation, and effectiveness of security controls (and, in some cases, controls over system availability, processing integrity, and the protection of confidential or private information used by the service organization's system. To support their risk assessments, customers and business partners may request a SOC 2® report from the service organization.

- **SOC for Cybersecurity.** As part of an entity's cybersecurity risk management program, an entity designs, implements, and operates cybersecurity controls. An engagement to examine and report on a description of the entity's cybersecurity risk management program and the effectiveness of controls within that program is a cybersecurity risk management examination.

Appendix A provides a comparison of SOC 1, SOC 2 and SOC for Cybersecurity.

SOC 1 Reports

SOC 1 reports are commonly used by service providers to employee benefit plans. As many of you know, there are two types of reports for these engagements:

- T*ype 1 SOC 1 report* is a report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.

- T*ype 2 SOC 1 report* is a report that also includes the service auditor's opinion on the operating effectiveness of the controls and a detailed description of the service auditor's tests of the operating effectiveness of the controls and the results of those tests throughout a specified period.

For plans that utilize service organizations for most (or all) of their electronic records and investment transactions, a common misconception may be that those plans have relatively little cybersecurity risk if the service organization's SOC 1 report identifies no issues. However, a SOC 1 report addresses only a plan's internal control over financial reporting; it does not address broader entity cybersecurity controls and risk.

SOC 2 Reports

A SOC 2 report, however, specifically addresses the cybersecurity risks that service organizations face and the controls they have implemented to mitigate those risks. The report may also address controls relevant to the service organization's ability to maintain the confidentiality or privacy of the information processed by the system. Therefore, a SOC 2 report can provide plan management with the information they need from the service provider to assess and manage the plan's risks associated with outsourcing functions to providers by providing information about the effectiveness of controls at the service organization and how those controls integrate with the plan's controls.

A SOC 2 examination and related control enables:

- Service organization management to prepare a description of the system (system description) to provide outsourced services to the plan. The system description also includes controls designed and implemented to mitigate security risks to the system and the information it processes.
- CPAs to perform a consulting engagement to help service organization management develop the system description
- CPAs to perform a consulting engagement known as a "readiness assessment" to help the service organization identify where its security controls may need to be shored up.

- CPAs to examine and report on a service organization's system description and the suitability of design and operating effectiveness of the security controls within that system

SOC 2 Criteria

A SOC 2 report is considered the gold standard for third-party risk management; the demand for SOC 2 reports continues to grow exponentially as users continue to value the trust and confidence that a CPA's involvement in a service organization's (or other third parties) efforts to protect its systems and information from breach.

Similar to a SOC 1 report, there are two types of SOC 2® reports:

- Type 1 SOC 2 report provides a CPA's opinion on whether:

    i. a service organization's description presents the system that was designed and implemented as of a point in time in accordance with the *description criteria* and
    ii. controls were suitably designed as of a point in time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable *trust services criteria,* if controls operated effectively.

- Type 2 SOC 2 report provides a CPA's opinion on the information in i. and ii. and also:

    iii. an opinion about whether controls stated in the description operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable *trust services criteria*.
    iv. a detailed description of the service auditor's tests of controls and the results of those tests.

A SOC 2 examination is performed by using criteria two sets of distinct but complementary criteria. Created specifically by the AICPA for use in SOC examinations, the description of the system and information about the effectiveness of security controls within that system provide intended users with the information they need to make data-driven decisions (for example, decisions around third-party vendor selection, vendor management, and risk assessment within their own organizations). The two criteria are:

> ***Description criteria.*** The *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022*), are used by management when preparing the description of the service organization's system (and by the service auditor when evaluating the description. A description of the service organization's system presented in accordance with the description criteria is designed to enable plan sponsors, administrators, business partners, and other intended users of the SOC 2 report to understand the service organization's system, including the processing and flow of data and information through and from the system. The description describes the procedures and controls the service organization has implemented to manage the security risks that threaten the achievement of the service organization's service commitments and system requirements.

Trust services criteria*.* The *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022*) (the 2017 trust services criteria), includes the criteria used to evaluate the suitability of design and operating effectiveness of controls stated in the description to provide reasonable assurance *that the service organization's service commitments and system requirements* were achieved. Based on the 2013 Internal Control — Integrated Framework developed by the Committee of Sponsoring Organizations of the Treadway Commission, the trust services criteria provide users and auditors with a common framework for evaluating security controls the service organization has implemented to address its security risks, which are unique to each organization.

Categories of Trust Services Criteria. The trust services criteria are classified into the following five categories:

- ***Security.*** **Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.**

- *Availability.* Information and systems are available for operation and use to meet the entity's objectives.

- *Processing integrity.* System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

- *Confidentiality*. Information designated as confidential is protected to meet the entity's objectives.

- *Privacy.* Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

When intended users are interested only in understanding a service organization's system and related security controls, service organization management and the CPA address only the common criteria, which consist of the following:

- Control environment
- Communication and information
- Risk assessment
    - Monitoring activities
    - Control activities. Control activities are further broken out into the following subclassifications:
    - Logical and physical access controls;
    - System operations;
    - Change management; and

When security is the only category addressed by the examination, no other criteria apply. When other categories are to be covered by the examination, the common criteria and the additional specific criteria for each category (availability, processing integrity, confidentiality, or privacy) need to be addressed.

SOC for Cybersecurity

Because the demand for reliable, comparable information about organization's cybersecurity efforts are increasing, the AICPA also developed a market-driven, flexible, and voluntary *entity-level* Cybersecurity Risk Management Reporting Framework (framework) through which organizations can communicate useful information about their cybersecurity risk management program. (As defined in the AICPA framework, a cybersecurity risk management program is a set of policies, processes, and controls 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.)

Such information may be useful to stakeholders, including boards of directors, analysts, investors, business partners, industry regulators, and others whose decisions are directly impacted by the effectiveness of an organization's cybersecurity efforts. The CPA's opinion on such information enables users to place confidence in the information the organization communicates about its cybersecurity measures. For example, a SOC for Cybersecurity report may be helpful to the following stakeholders:

- Senior management, who wants information about the effectiveness of an organization's cybersecurity risk management program, including the controls designed, implemented, and operated to mitigate threats against the entity's sensitive information and systems.

- Boards of directors, who want information about the cybersecurity risks the entity faces and the program that management has implemented to help them fulfill its oversight responsibilities and to help them evaluate management's effectiveness in managing cybersecurity risks.

- Business partners, who want information about an entity's cybersecurity risk management program to help them with their overall risk assessment. This information may help determine matters such as whether there is a need for multiple suppliers for a product or service and the extent to which they may choose to extend credit to the entity. Other business partners may need a detailed understanding of controls implemented by the entity and the operating effectiveness of those controls to enable them to design and operate their own control activities. For example, business partners whose IT)systems are interconnected with systems at the entity may need to understand the specific logical access protections over the interconnected systems implemented by the entity.

The AICPA's framework provides a common, underlying language for cybersecurity risk management reporting, almost akin to US GAAP or IFRS for financial reporting, to enable all organizations – in all industries – to communicate relevant information about their cybersecurity risk management programs to interested parties. Use of a common language brings comparability to the disclosures and enhances and complements disclosures based on other commonly used security frameworks, such as NIST or ISO's

27001. Recognizing that cybersecurity is not just an IT issue, the framework is a robust reporting framework and related criteria that can be used by organizations to enhance cybersecurity risk management reporting and by CPAs to examine and report on such information.

The AICPA cybersecurity risk management framework creates opportunities for:

- Plan management to describe the plan's cybersecurity risk management program.
- CPAs to perform a consulting engagement to help plan management develop a description of the plan's cybersecurity risk management program to provide to the board and other internal parties who are interested in that information.
- CPAs to perform a consulting engagement known as a "readiness assessment" to help plan management identify where the plan's cybersecurity processes and controls may need to be shored up. In addition, the AICPA has introduced SOC for Cybersecurity, which:
- Enables CPAs to examine and report on a plan's cybersecurity risk management program.
- Results in the issuance of a general-use cybersecurity report designed to meet the needs of a variety of potential users.

The SOC for Cybersecurity report includes the following three key components

- Management's description of the entity's cybersecurity risk management program prepared in accordance with DC section 100, *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program***.** The description is designed to provide information about how the entity identifies its information assets, the ways in which the entity manages the cybersecurity risks that threaten it, and the key security policies and processes implemented and operated to protect the entity's information assets against those risks. The description provides the context needed for users to understand the conclusions, expressed by management in its assertion and by the practitioner in his or her report.

- Management's assertion. The report includes an assertion provided by management, which addresses whether (a) the description is presented in accordance with the description criteria and (b) the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria. The 2017 trust services criteria may be used as the measurement criteria; however, other criteria considered suitable for the examination may also be used to evaluate the effectiveness of cybersecurity processes and controls.

- CPA's report. The report also includes a CPA's opinion that addresses the same matter addressed by management's assertion.

A SOC for Cybersecurity report is appropriate for general use.

Summary

Employee health benefit plans, like other organizations, need to understand how service organizations to which they have outsourced services are managing their cybersecurity risks. As discussed earlier, when realized those risks can have devasting consequences not only to the plan but also to the plan sponsor, administrator and even plan participants.

SOC 2 reports can provide information to plan management to enable them to understand the service organization's systems, as well as the effectiveness of security controls within that system, to assist them with their own security efforts. SOC for Cybersecurity can provide useful information to a broad range of stakeholders about the effectiveness of an organization's entity-wide cybersecurity efforts. CPA involvement with cybersecurity information provided by service organizations and others can enhance the value that users can place on that information, much like a CPA's opinion on audited financial statements enhances the value of that information to analysts, investors, regulators, bankers, and others who rely of them for decision making.

Thank you for the opportunity to present our views and recommendations.