Testimony of
Daniel Nutkis, CEO
HITRUST

Before the Advisory Council on Employee Welfare and Pension Benefit Plans
August 24, 2016

Prepared for Submission

Good morning Chairman Schmidtke, Vice Chairwoman Tretheway, and members of the Council. I am pleased to appear today to discuss the role of cybersecurity in the administration of Employee Welfare and Pension Benefit Plans, and how initiatives underway by HITRUST and the healthcare industry can help these Plans implement robust cybersecurity programs and provide for risk-based protection of the sensitive information they hold.

I am Daniel Nutkis, Chief Executive Officer and founder of the Health Information Trust Alliance, which is more commonly known as HITRUST. Founded in 2007—after recognizing the need to formally and collaboratively address information privacy and security for healthcare stakeholders representing all segments of the industry, comprising health plans, providers, pharmacies, PBMs, exchanges and manufacturers—HITRUST endeavored, and continues to endeavor, to efficiently and effectively elevate the level of information protection in the healthcare industry, ensure greater collaboration between industry and government, and raise the competency level of information security professionals in healthcare.

I'll provide more information on relevant HITRUST programs and services as I address the privacy and security issues affecting employee benefits raised in the Council's 2011 report on *Privacy and Security Issues Affecting Employee Benefit Plans*;[1] address some of the elements of a scalable cyber risk management strategy for benefit plans provided in its scoping document,[2] *Cybersecurity Considerations for Benefit Plans*; and make specific comments and recommendations on the current draft *Guidance on Navigating Cybersecurity Risks*[3] for employee benefit plans.

A precursor to the draft guidance, the Council's 2011 report on privacy and security issues recognizes that the protection of personally identifiable information, or PII, is a fiduciary responsibility of plan sponsors and administrators. At the same time, the Council recognizes that

[1] Advisory Council on Employee Welfare and Pension Benefit Plans (November 9, 2011). Privacy and Security Issues Affecting Employee Benefit Plans: Report to the Honorable Hilda L. Solis, United States Secretary of Labor. Washington, DC: Author. Retrieved from https://www.dol.gov/ebsa/pdf/2011ACReport2.pdf.

[2] Advisory Council on Employee Welfare and Pension Benefit Plans (n.d.a). Cybersecurity Considerations for Benefit Plans. Washington, DC: Author.

[3] Advisory Council on Employee Welfare and Pension Benefit Plans (n.d.b). Guidance on Navigating Cybersecurity Risks (DRAFT). Washington, DC: Author.

many organizations are subject to extensive regulation or other legal requirements that result in multi-faceted efforts to protect PII, resulting in higher costs due to inefficiencies and higher risk due to the inconsistent application of security safeguards across the organization.

Healthcare organizations are also subject to a multitude of regulations, standards and other policy requirements, as well as commonly accepted best practice frameworks, for the protection of personally identifiable health information, which the Health Insurance Portability and Accountability Act, or HIPAA, refers to as Protected Health Information, or PHI. However, these 'authoritative sources' often overlap in the depth and breadth of their requirements, which can lead to duplication and other inefficiencies, but when intelligently applied in the intended environment can be mutually reinforcing.

The HITRUST CSF—a core component of the HITRUST risk management framework (RMF)—integrates and harmonizes these authoritative sources into a single comprehensive, prescriptive, yet flexible security and privacy framework that can be used by all types of healthcare organizations, including health plans and third-party administrators, both large or small. The HITRUST CSF is also updated at least annually to ensure it remains relevant to the changing healthcare threat environment. The review takes into account changes in underlying regulations and standards and also considers best practices and lessons learned from security incidents, incident response exercises, and industry post data breach experiences.

This level of comprehensiveness, relevance, and applicability is why over 80 percent of hospitals and health plans, as well as many other healthcare organizations and business associates, have adopted the HITRUST CSF, making it the most widely used privacy and security framework in the industry. This broad acceptance of the HITRUST CSF also provides the healthcare industry a de facto standard of due diligence and due care for the appropriate protection of PHI.

The Council's 2011 report also recognizes that "an appropriate standard of due diligence [should] be used to evaluate controls over the security and privacy of the PII of plan participants and beneficiaries, especially since this information is such a critical part of the operation of the plan and its protection is so important to the welfare of plan participants."[4] As with the myriad of applicable regulation, standards and best practices, the healthcare industry is also subject to a similar level of due diligence by HIPAA, which requires covered entities, including health plans and third party administrators, to obtain satisfactory assurances from its business associates around the protection of the PHI to which they have access.

Another part of the HITRUST RMF, the HITRUST CSF Assurance Program, delivers a comprehensive, consistent, and simplified compliance assessment and reporting program for regulatory requirements, such as HIPAA, HITECH, and other federal and state requirements, and the sharing of assurances between and amongst covered entities and business associates. Specifically designed for the unique regulatory and business needs of the healthcare industry, the CSF Assurance Program provides healthcare organizations and their business associates with a

[4] Advisory Council on Employee Welfare and Pension Benefit Plans (November 9, 2011), p. 8.

common approach to manage privacy and security assessments that enables efficiencies and contains costs associated with multiple and varied information protection requirements. The CSF Assurance Program also incorporates specific guidelines to allow a broad array of leading industry professional services firms to perform services, while allowing HITRUST to oversee quality assurance processes to ensure assessments are rigorous, consistent, and repeatable.

An additional benefit of using the HITRUST RMF is that it supports assessment and reporting against a common control framework for multiple and varied purposes, such as the evaluation; reporting 'scorecards' against regulatory requirements and best practice frameworks, such as HIPAA and the Payment Card Industry Data Security Standard (or PCI-DSS); and certification against State-based covered entity privacy and security programs, such as SECURETexas.[5] In addition, the American Institute of Certified Public Accountants (AICPA) has recognized the HITRUST CSF as an acceptable citeria and established guidance for Trust Services Principles and Criteria and SSAE-16 SOC 2 reporting, [6] which is being used extensively by many health plans to address their SOC 2 reporting requirements.

And the need to ensure the appropriate safeguarding of health information by business partners continues to be a significant undertaking. This is true for both the organization requiring compliance by its business partners and the organization having to demonstrate compliance. This issue is only magnified by recent cyber-related events, the provisions of the HITECH Act and the omnibus HIPAA privacy and security rule, the proliferation of disparate state and federal regulations, and the disproportionally high number of data breaches by business partners.

Various approaches relying on inconsistent and uncoordinated requirements have also led to similarly inconsistent and uncoordinated assessments with associated high costs and taxed resources of the entity being assessed. HITRUST documented instances where individual business associates were receiving over 1,000 privacy and security assessment or attestation requests annually, requiring tens of thousands of man hours to appropriately respond. The industry recognized that a more efficient approach to third-party assurance is needed, and it is believed the recent adoption of the CSF Assurance Program as the basis for vendor risk management programs by numerous health plans[7] will go a long way in streamlining the process for both the organization requesting the assessment and the organization being assessed.

A growing number of other healthcare organizations are aligning their vendor risk management requirements by leveraging the HITRUST CSF Assurance program and establishing similar expectations with their vendors regarding CSF assessment and certification. This alignment

[5] SECURETexas is the first state program of its kind in the country offering privacy and security certification for compliance with state and federal laws that govern the use of protected health information (PHI).

[6] Healthcare organizations have been saving roughly 25-30% of audit costs when leveraging a HITRUST RMF Certification and a SSAE-16 SOC2 audit. Similar underwriting and auditing savings are also envisioned as the cyber insurance industry matures.

[7] HITRUST (Jun3 29, 2015). CSF Assurance Program Adoption Key to More Effective Third-Party Risk Management in the Healthcare Industry (Press Release). Retrieved from https://hitrustalliance.net/csf-assurance-program-adoption-key-to-effective-third-party-risk-management

enables a single assessment to be accepted by many organizations across the industry and reduces the resource requirements and costs associated with redundant assessments.

But even if an organization implements a robust security and privacy program and obtains the necessary assurances from its business partners that they can and will protect its PII, there is no guarantee that a data breach won't occur. In fact, the Council states in its draft guidance on cybersecurity that "it's not a question of 'if' you will have a cyber-attack, it's a question of 'when' and 'what' you're going to do about it."[8] This position is supported by a marked increase in the use of electronic information and a resulting increase in the level of exposure to cyber-attacks across multiple critical infrastructure industries over the past several years, including healthcare.

A data breach in the healthcare industry not only has financial and reputational effects on the company targeted by the threat actors, but the effects could be dramatic for members, patients, and their families due to the nature of the data disclosed. Personal health information or identities could be stolen directly from hospitals, insurance companies, pharmacies and from any business associate supporting these organizations. Beyond the privacy implications of data breach incidents, these breaches have the potential to disrupt operations of a healthcare facility or affect patient care. The various complexities, interdependencies, and unique attributes all create various risk levels that need to be considered by healthcare organizations across the continuum of care.

Subsequently, HITRUST believes it's in the best interests of an organization to adopt a cyber 'resilience' approach to cybersecurity, such as the one posited by the National Institute of Standards and Technology, or NIST, *Framework for Improving Critical Infrastructure Cybersecurity*,[9] more commonly known as the NIST Cybersecurity Framework. President Barack Obama directed NIST to work with the private sector and develop the Cybersecurity Framework[10] to reduce cyber risks to critical infrastructure, including a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. In doing so, NIST recommended that organizations base their cybersecurity programs on five core function areas: Identify, Protect, Detect, Respond and Recover. By placing equal importance on incident response and recovery as on identifying and protecting one's information assets, the NIST Cybersecurity Framework helps organizations quickly respond to security incidents, reduce the frequency of data breaches, and minimize the impact of data breaches should they occur.

It's clear to HITRUST that the Council recognizes that data breaches will occur and that benefit plans must adopt a resilience approach to its cybersecurity programs, as the Council's draft *Guidance on Navigating Cybersecurity Risks* specifically adopts the NIST Cybersecurity Framework's five Core Functions as the basis of its recommended cybersecurity strategy. However, simply specifying a cybersecurity strategy will only provide limited benefits to

[8] Advisory Council on Employee Welfare and Pension Benefit Plans (n.d.b). Guidance on Navigating Cybersecurity Risks (DRAFT). Washington, DC: Author, p. 1.

[9] NIST (February 12, 2014). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. Gaithersburg, MD: Author. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[10] Exec. Order No. 13636, 3 C.F.R. 11739-11744 (2013). Retrieved from http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

adopting organizations. HITRUST therefore recommends that the Council adopt the same approach for Employee Welfare and Pension Benefit Plans as the healthcare industry did for covered entities and business associates, including health plans and their subcontractors, and vendors who have access to PHI.

In addition to NIST's development of the Cybersecurity Framework, the President also called on Sector-specific Agencies to "coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments."[11] The Joint [Sector Coordinating Council and Government Coordinating Council] Healthcare and Public Health (HPH) Cybersecurity Working Group (WG) subsequently launched a Risk Management (RM) Sub-working Group (SG) in 2015, co-chaired by HITRUST and the Office of the National Coordinator for Health Information Technology, to build upon the work of existing organizations within the HPH Sector to further advance implementation of the high-level guidance provided in the Cybersecurity Framework.

Developed by the RM SG for the Joint HPH Cybersecurity WG, the *Healthcare Sector Cybersecurity Framework Implementation Guide*[12] seeks to help organizations understand and use the HITRUST RMF to achieve the goals of the NIST Cybersecurity Framework and support implementation of a sound cybersecurity program that addresses the Framework's five Core Function areas to ensure alignment with national standards, help organizations assess and improve their level of cyber resiliency, and provide suggestions on how to link cybersecurity with their overall information security and privacy risk management activities to the HPH Sector.

The healthcare sector guide presents background information on the NIST and HITRUST frameworks, including potential benefits to HPH Sector organizations, explains the relationship between the two frameworks and how the HITRUST RMF provides a model implementation of the NIST Cybersecurity Framework for the healthcare industry, presents a mapping of HITRUST CSF controls to the NIST Cybersecurity Framework's Subcategories, and provides additional implementation guidance. The sector guide also helps an organization's leadership:

- Understand NIST Cybersecurity Framework and HITRUST RMF terminology, concepts, and benefits
- Assess their current and targeted cybersecurity posture
- Identify gaps in their current programs and workforce, and
- Identify current practices that exceed NIST CsF requirements

Other benefits of the HITRUST RMF are provided through CSF-related programs such as the HITRUST De-Identification Framework, including practical training and practitioner certification, as well as operational cybersecurity support, such as the sharing of threat

[11] Ibid.

[12] Joint HPH Cybersecurity WG. (May 2016). Healthcare Sector Cybersecurity Framework Implementation Guide, Version 1.1. Washington, DC: Author. Retrieved from https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf.

information and collaboration with industry and government organizations on incident response exercises at the local, regional and national levels.

If the Council fully embraces the NIST approach to cybersecurity beyond a high-level strategy and adopts current HPH Sector guidance for implementation of the NIST Cybersecurity Framework through application of the HITRUST RMF—specifically the HITRUST CSF and the CSF and Third-party Assurance Programs, including SOC2 for HITRUST—benefit plans would benefit immediately since much of the heavy lifting for cybersecurity has already been done. The HITRUST RMF can be adopted by non-healthcare benefit plans as the HITRUST CSF controls are broadly applicable to many types of sensitive information, including PII. HIPAA requirements specific to PHI would simply be marked "not applicable" and not included in the organization's cybersecurity program requirements nor considered when conducting assessments. And neither the Council nor the benefit plans would need to "re-invent the wheel" and introduce unnecessary complications, inefficiencies and costs into the benefit plans' cybersecurity programs, especially for those benefit plans considered covered entities under HIPAA.

And now I'd like to address specific issues raised in the Council's scope document entitled *Cybersecurity Considerations for Benefit Plans* and provide specific comments and recommendations on the draft *Guidance on Navigating Cybersecurity Risks*.

Specific Comments on *Cybersecurity Considerations for Benefit Plans*

HITRUST agrees that there appears to be some commonality between retirement and health and welfare plans for the reasons cited in the scoping document, and our responses will apply generally to both.

A. *As background, review the general types of cybersecurity risks that benefit plans are exposed to and how the overall threat environment is evolving.*

   Response: Benefit plans are generally exposed to the same dynamic threat environment as health plans, which may hold ePHI, PII and financial data (e.g., payment card data subject to PCI DSS). The HITRUST CSF is specifically designed to address these threats, and is updated no less than annually to ensure the controls remain relative to extant and emerging threats. The HITRUST CSF also provides the foundation for healthcare sector guidance on cybersecurity.

B. *Obtain information about the steps, processes and controls that plans and third-party providers are taking to address these risks.*

   Response: As with health plans before the creation of HITRUST by the healthcare industry, we believe benefit plans struggle to determine an effective cybersecurity approach let alone one that is consistent amongst plans and provides a generally accepted level of due diligence and due care. Adoption of the recommendations contained in the *Healthcare Sector Cybersecurity Framework Implementation Guide* will ensure benefit plans take a consistent approach to risk management and regulatory compliance and provide for the adequate protection of the sensitive information they hold.

C. *Examine how cybersecurity risks and exposure differ between small plan sponsors and large plan sponsors, with the objective of tailoring guidance and education accordingly.*

Response: The HITRUST CSF parses control requirements amongst up to three implementation levels and multiple industry segments for specific entity and data types, the selection of which is based on three types of risk factors: organizational, system, and regulatory. The intent is to ensure an equivalent amount of residual risk is maintained by differing types of entities, e.g., large vs. small.

D. *Draft materials that may help plan sponsors identify and establish a scalable cyber risk management strategy.*

Response: The structure of the HITRUST CSF and the selection of CSF controls based on organizational, system, and regulatory risk factors provide direct support for a scalable cyber risk management strategy. This strategy is also supported by the ability of an organization to implement alternate (or compensating) controls in lieu of the standard control requirements specified in the CSF as well as the ability of an organization to accept small amounts of excessive residual risk. If HITRUST CSF certification is not required, the organization has even more flexibility to manage and accept risk, the specifics of which would be indicated in a HITRUST validated assessment report or a SOC 2 for HITRUST report.

E. *Draft materials that may help plan sponsors incorporate cybersecurity risk management in the vendor selection and monitoring process.*

Response: The HITRUST CSF specifically requires third-party risk management in the vendor selection and monitoring process via CSF control objective 05.02 External Parties, which is supported by CSF controls 05.i Identification of Risks Related to External Parties, 05.j Addressing Security When Dealing with Customers, and 05.k Addressing Security in Third Party Agreements.

F. *Invite interested parties to submit sample tip sheets, checklists and other educational tools that can be used to provide plan sponsors, vendors and plan participants with guidance on navigating cybersecurity risks related to their benefit plans.*

Response: HITRUST provides the following resources, among others, that the Council may find of interest:

- HITRUST CSF v8 and supporting documentation (no cost via public license). https://hitrustalliance.net/csf-license-agreement/
- Selecting a Healthcare Information Security Risk Management Framework in a Cyber World. https://hitrustalliance.net/content/uploads/2016/01/HCSC_Childrens_Health_Selecting_Healthcare_Information_Security_RMF_in_a_Cyber_World.pdf

- Healthcare Sector Cybersecurity Framework Implementation Guide. https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf
- Risk Analysis Guide for HITRUST Organizations and Assessors. https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf
- Understanding HITRUST's Approach to Risk vs. Compliance-based Information Protection. https://hitrustalliance.net/documents/csf_rmf_related/RiskVsComplianceWhitepaper.pdf
- Leveraging HITRUST CSF Assessment Reports – A Guide for New Users. https://hitrustalliance.net/documents/assurance/csf/Leveraging_2016_CSF_v8_Assessment_Reports.pdf

Specific Comments on draft *Guidance on Navigating Cybersecurity Risks*

A. *Does your plan have a cybersecurity strategy?*

Response: The NIST Cybersecurity Framework provides a general cybersecurity strategy but additional specificity is required for an organization to implement the Framework's recommendations. This is the role of the *Healthcare Sector Cybersecurity Framework Implementation Guide*, which addresses the goals and objectives of the NIST guidance through the HITRUST RMF, including the HITRUST CSF and CSF Assurance Program.

B. *What are the components of a cybersecurity strategy?*

1. *Describe a process to identify risks*
2. *Develop a program to protect data that could be at risk*
3. *State how breaches will be detected*
4. *Show how your plan will be able to respond*
5. *Detail how your plan will recover*

Response: The NIST Cybersecurity Framework's Core Functions used as the basis for the Council's cybersecurity strategy provides for a cyber resilience approach to cybersecurity risk management, as it recognizes that incident detection, response and recovery are needed, in addition to identifying and protecting one's assets, to help ensure an organization can minimize the risk to operational and strategic objectives should a security incident and/or data breach occur. The HITRUST CSF addresses each of the five Core Functions (identify, protect, detect, respond and recover) in significant detail, providing the prescription necessary for any organization to implement a cyber risk management program that (1) identifies its most sensitive and critical business assets, (2) prioritizes protection based on sensitivity and criticality, (3) expects and anticipates cyber breaches, and (4) implements response and recovery plans that minimize reputational, financial, operational, and regulatory compliance impacts. For more information on how the HITRUST CSF supports each of the NIST Functions, Categories and Subcategories (essentially control objectives), I refer you to the HITRUST CSF Authoritative Sources Cross-reference spreadsheet available in the CSF download package identified earlier.

C. *Establishing a cybersecurity strategy.*

Response: HITRUST addresses an organization’s cybersecurity strategy in CSF Control Category 0.0 and CSF Control 0.a, entitled Information Security Management Program, and CSF Control Category 03.0 Risk Management, which is supported by CSF control 03.a Risk Management Program Development, 03.b Performing Risk Assessments, 03.c Risk Mitigation and 03.d Risk Evaluation. These controls ensure the organization develops an appropriate strategy for identifying critical assets, specifying controls to protect and mitigate the risk to those assets, detecting and responding to threats as they materialize, and recovering assets and processes to normal operations.

D. Understanding your data.

1. *What is it? Participant data can contain sensitive personally identifying information that is made available to various parties multiple times. This data may include Social Security Numbers, Names, Dates of Birth, Dates of Hire and Compensation.*

   Response: The HITRUST CSF is designed to protect different types of information that have similar sensitivity and criticality requirements, such as PII, PHI and payment card data. CSF control 07.a addresses the Inventory of Assets, 07.d provides Classification Guidelines, and 07.e addresses Information Labeling and Handling. The HITRUST CSF also provides requirements around limited and de-identified data sets as well as information types that require special handling, e.g., HIV and mental health data.

2. *What type of Plan do you have? Plan type affects the kinds of data at risk. For example, defined contribution retirement plans have individual asset balance information whereas health and welfare plans track medical claims data. Also, plans may have personal bank account details*.

   Response: See my response to D.1 above.

3. *Where is your data stored? Multiple parties handle benefit plan data. It is important to understand where it is, how it is being stored, and the retention period.*

   Response: The HITRUST CSF addresses an organization’s Inventory of Assets in CSF control 07.a; storage requirements in multiple controls such as CSF control 08.c Securing Offices, Rooms, and Facilities, 08.g Equipment Siting and Protection, 08.l Secure Disposal or Re-use of Equipment, and 09.o Management of Removable Media, among others; and retention is specifically addressed in CSF control 06.c Protection of Organizational Records.

4. *How is it being accessed and who is accessing it? Benefit plan data is shared across multiple parties as a part of the plan administration process. It also may*

be linked to other unrelated system that hackers access. Plan sponsors and administrators should understand how benefit plan data is being shared, accessed and kept secure.

Response: HITRUST CSF Control Category 1.0 is devoted to Access Control, and is supported by 25 controls that address CSF Control Objectives for 01.01 Business Requirements for Access Control, 01.02 Authorized Access to Information Systems, 01.03 User Responsibilities, 01.04 Network Access Control, 01.05 Operating System Access Control, 01.06 Application and Information Access Control, and 01.07 Mobile Computing and Teleworking access.

5. *How is it classified? Benefit plan data sometimes has special classifications. Specific standards of care apply to different types of data. Examples include Personally Identifiable Information (PII) and Personal (sic) Health Information (PHI).*

   Response: HITRUST CSF control 07.d provides Classification Guidelines and 07.e addresses Information Labeling and Handling, including the handling of special access information.

E. What processes are needed to support your cybersecurity strategy?

1. *Who is responsible for implementing your strategy?*

   Response: Responsibilities are specified in HITRUST CSF Control 05.a Management Commitment to Information Security, 05.c Allocation of Information Security Responsibilities, and 06.d Data Protection and Privacy of Covered Information.

2. *Is your strategy reviewed regularly?*

   Response: Requirements for the regular review of the information security program, including its strategy, are addressed in HITRUST CSF control 0.a, Information Security Management Program, 03.d Risk Evaluation, and 05.h Independent Review of Information Security. HITRUST CSF Control 04.b requires Review of the Information Security Policy.

3. *Are your cybersecurity procedures tested periodically and updated as needed?*

   Response: The HITRUST CSF Assurance Program implements a robust approach to continuous monitoring by evaluating each control requirement for a relevant metric and management response should the metric indicate a loss of effectiveness. The HITRUST CSF also addresses specific cybersecurity incident response testing in CSF Control 11.b Responsibilities and Procedures and incorporating lessons learned in 11.d Learning from Information Security

Incidents.

4. *Are reports to fiduciaries made regularly and memorialized in official records?*

   Response: General reporting is addressed in CSF Control 04.a Information Security Policy Document, reporting to external stakeholders such as law enforcement is addressed in 05.f Contact with Authorities, reporting requirements for third parties is outlined in 05.k Addressing Security in Third Party Agreements, internal reporting is addressed by 06.g Compliance with Security Policies and Standards, and incident and breach reporting is addressed in 11.a Reporting Information Security Events.

5. *Does your strategy include training? Training is critical – users are the weakest link.*

   Response: Training of users and security personnel is addressed extensively by CSF Control 02.e Information Security Awareness, Education, and Training.

6. *Do you know who your users are? Does your strategy include getting rid of unnecessary data? A "data diet" reduces cyber risk.*

   Response: Unique identification of users is addressed in CSF Control 01.b User Registration and 01.q User Identification and Authentication. The unique identification of users in audit logs is required in CSF Control 09.aa Audit Logging. Retention and disposal of data is addressed in CSF Control 06.c Protection of Organizational Records. The requirement to limit the data stored and associated retention to that which is required for business is specifically required in CSF Control 06.d Data Protection and Privacy of Covered Information.

F. What strategy fits your plan?

1. *How large is your plan's administrative budget, and how much can be spent on your cyber security strategy?*

   Response: Defining security requirements and programming and budgeting for security is specifically addressed in CSF Control 05.b Information Security Coordination.

2. *If your plan experiences a breach without an effective cyber security plan, how much can you afford to spend on dealing with a breach?*

   Response: Refer to the response for F.1 above.

3. *What's the balance between the two?*

   Response: This is a decision that is unique to an organization and can only be made by organizational leadership.

4. *Have you considered cyber insurance or commercially available resources or tools?*

   Response: Consideration for suitable insurance is addressed in CSF Control 12.a Including Information Security in the Business Continuity Process. HITRUST is also working with the insurance industry to support underwriting based on the results of HITRUST CSF validated assessments; Allied World was the first insurance company to offer discounts to HITRUST CSF certified organizations.

5. *How much is enough to address your risks while being affordable?*

   Response: This is a decision that is unique to an organization and can only be made by organizational leadership.

G. *(TPA Insert) If you contract with a TPA for plan administration, does your contract include:*

1. *The TPA's description of its cybersecurity program*
2. *The elements of their program*
3. *A statement of how your data will be maintained and protected*
4. *An agreement that your data will be encrypted*
5. *An agreement on liability for breaches*
6. *A statement of permitted use and restrictions on use*
7. *Agreed protocols for notifications and plan management in the case of a breach.*
8. *A description of regular reports and monitoring*
9. *A requirement of external reviews of controls, such as SOC (Type 1, 2) or similar report*
10. *The level and coverage of cyber insurance that is available to you in case of a breach.*
11. *The level of financial and fraud coverage that protects against financial damage to participants*
12. *If TPA subcontracts to others, all of above should be included in the subcontract.*

Response: Specific requirements such as those outlined above are addressed by CSF Control 05.k Addressing Security in Third Party Agreements.

H. *(Cyber Insurance Insert) Have you considered cyber insurance?*

1. *Do you know exactly what is included and what is excluded from your cyber insurance policy?*
2. *Have you reviewed what is covered by other insurance such as fiduciary insurance and what the gaps and overlaps in coverage may be?*
3. *Do you know what coverage is available to you in the case of a breach and what is the cost?*

4. *Do you fully understand and can you comply with the policy terms and conditions of coverage?*
5. *Does the coverage include protection for participants against financial damage in the case of a breach?*
6. *Does the policy cover breaches of other third-party providers?*
7. *Have you reviewed the policy terms for loopholes and ambiguous provisions?*
8. *Does the policy cover breaches by service providers?*
9. *Does the policy cover third-party action or direct first-party coverage or both?*

Response: The HITRUST CSF does not currently address specific requirements for cyber insurance other than to specify consideration for its purchase. Requirements such as those specified in the Council's draft guidance (above) could easily be incorporated into a suitable CSF control, such as 12.a Including Information Security in the Business Continuity Process.

Closing Remarks

I hope it is clear from the testimony provided that HITRUST has been evaluating, engaging and addressing the very same issues as the Council within the healthcare industry, and the HITRUST RMF—consisting of the HITRUST CSF and CSF Assurance Program, including a myriad of Third Party Assurance Program components—provides a time-tested and industry-vetted cybersecurity framework and an efficient and effective assurance approach that has been demonstrated to be a model implementation for the healthcare industry.

It should also be clear that many benefit plans—large and small—are already leveraging the HITRUST RMF to build out their own cybersecurity programs and avoid unnecessary duplication, complexity and cost. Thorough consideration needs to be given to the implications of imposing additional requirements in the way of controls, assessments and reporting on health plans that introduce additional costs or distract resources from implementing and monitoring their cybersecurity programs.

Therefore, our recommendation for the Council is that plan sponsors require a HITRUST CSF Certification or a SOC 2 leveraging the HITRUST CSF controls as a means of evaluating and determining the effectiveness of the privacy and security programs of health plans, third-party administrators and other organizations that create, store or exchange PHI of a plan sponsor in lieu of another approach that would create inefficiencies and duplication.

On behalf of the HITRUST Community, I would like to thank the Advisory Council for the opportunity to provide these comments on its general approach to cybersecurity and specifically the draft *Guidance on Navigating Cybersecurity Risks* for employee welfare and pension benefit plans, and we look forward to working with the Council to make the guidance a success.