Good morning, and thank you for the opportunity to speak with the Committee today. My name is Tom Doughty, Vice President & Chief Information Security Officer at the Prudential Insurance Company of America. From our senior most executive management down through the organization, Information and Cyber Security represents a focus and commitment at Prudential, and we see it as a fundamental tenet of our fiduciary responsibility to our supported Sponsor and Participant base.

I'd like to offer some thoughts and insight from the industry perspective in terms of what Providers, Sponsors, and Participants can and should be thinking about and acting upon to ensure that collectively, we maintain a secure and responsibly operated environment.

Operating as Enterprises at the Provider and Sponsor levels, there's a lot of commonality in terms of key points. There is often discussion of "maintaining the moat" versus "the perimeter is gone" in terms of Cybersecurity. Both are true. We observe continual evolution of the threat profile, and therefore drive continual evolution of controls and associated prevention, detection, and remediation measures. However, this is not a zero sum question. Within effective Provider and Sponsor programs, the equation represents ongoing growth in applied resource and attention. Essentially, most of the legacy "perimeter" controls must remain, endure, and be diligently maintained. At the same time, more creative and aggressive anomaly detection, analytics, and threat / vulnerability management techniques and skill sets represent incremental, necessary investments. We recognize this, and are committed to commensurate attention and judicious investment.

I'd now like to describe three key commitments that both Providers and Sponsors should maintain as the basis for a solid, sustainable, and constantly evolving program of protections:

- The first is **MAKING SECURITY A BUSINESS IMPERATIVE**. While many points of monitoring, detection, protection and response in the Cybersecurity and privacy space are in fact technical in nature, the fact is that security, privacy, and the fiduciary responsibility to protect Sponsors and Participants is first defined as a business requirement. Strategic and tactical business decisions must be considered with security implications as core to the discussion. Security is something integral done within the business operation, not separately for the business operation. I often describe this as having an internally engaged security program down to the individual business operational and process level-- is there a security officer with a "seat at the table" at each tier of the organization, effectively organized and empowered to help drive security and participant protection considerations as a partner to the accountable business leaders? Is that person effectively integrated with complimentary governance functions including Privacy, Compliance, Operational Risk, Legal, and Audit? Can this person articulate security threat, control, and residual risk points in non-technical language in terms of business and consumer impacts which

the accountable business leaders already feel a duty to directly address? These litmus test questions often indicate for me whether or not an organization has the cultural and organizational basis for a strong, business and consumer focused program, whether introspectively or as part of performing external due diligence. I believe that these questions can serve equally well as litmus tests for Providers and Sponsors in general. In the end, a supporting Enterprise's security program must be solidly bolted to its mature risk management processes. This ensures that that the right residuals are articulated with the consumer interest in mind, and that these residuals are clearly owned and overseen by the right accountable business leaders.

- Secondly, Providers and Sponsors should programmatically **PROTECT WHAT IS IMPORTANT, DETECT INCIDENTS, AND RESPOND EFFECTIVELY**. This begins with understanding what the important informational and operational assets are. Is this exclusively a matter of participant account and personal information? While such information does of course represent one "crown jewel" to be protected, there are others including intellectual property, business strategy information, algorithmic data, etc, as examples which must be creatively identified and addressed with adaptive protections in order to protect the efficient operating environment within which Providers support every Participant. This "what are we protecting and why" discussion relates very closely to the tenet of making security a business imperative. Security professionals and technical professionals are good at architecting and implementing technical protections-- however, continual and contextual discussion between security leaders and accountable operational business leaders is crucial to focus such protections. These exchanges define in business terms the emerging or morphing business activities, use cases, sponsor or participant data or requirements, etc. against which we match new control options. Only from there may an effective technical portion of the program properly tailor and evolve preventative, detective, and response tools and process. From there, I would simply add that while continual introspective consideration of detection mechanisms and response processes is part of the deliverable-- there is no substitute for external validation of these measures through multi-faceted penetration testing and third party evaluation of every program.

- Based upon this continual cycle of considering business imperatives anchored in Participants' interest, and upon both internal and external observations upon which to adjust, every effective security program must **OBJECTIVELY EVALUATE AND CONTINUOUSLY IMPROVE**. Cybersecurity is an arena where we are never done, and where there is no room for complacency. External collaboration is critical in terms of threat intelligence and methodologies, both with peer Enterprises and with public sector agencies. I do not see competitive advantage in security, and it is to the benefit of Participants that Sponsors and Providers actively collaborate and share information to protect the collective environment. With that in mind, it's important to

also consider that technical tooling and information to protect operations, data, and participant interests is only as effective as the human capital invested in operating it. The skill sets required to "look beyond the headlights", not only in maintaining these protective technologies, but in tuning them, effectively reacting to and analyzing their outputs, and liaising with the underlying business functions are in growing and constant demand. As such, part of my message today is to urge Providers and Sponsors to consider their talent pipeline and investment in Cybersecurity talent as a proactive, long range endeavor as opposed to a role by role, short term set of tactical requirements.

Before addressing some thoughts around where Participants can and should focus in this space, I'd like to transition by referring to an illustration profiling the primary categories of threat actors in Cybersecurity and where their interests often lie:

Actor	**Target**
Nation States	• Business plans • Trade secrets • Insider Information • Causing Havoc at a time of international conflict
For-Profit Hackers	• PII • Credit card & bank account numbers • Personally Identifiable Information • M&A data for insider trading, negotiation advantage
Hacktivists	• Disruption of operation • Embarrassment via website defacement
Insiders	• For profit theft of intellectual property • Disruption of critical systems • Focus area for users with privileged access

From there, I describe three essential categories of threat that Providers and Sponsors face as Enterprises, but that Participants also face either directly or derivatively.

- The first is the **EXTERNAL THREAT**, which is often popularly embodied in terms such as "zero-day threat" or "Advanced Persistent Threat (APT)". The fact of the matter is, whether an attack or exploit is new versus previously unseen... or whether it is targeted versus generalized in nature...

many of them are neither advanced nor persistent. Advanced technologies and tools to detect previously unseen anomalies, compare them to other similar observations within and beyond our Enterprise boundaries, and respond appropriately have grown in effectiveness and continue to become more powerful. That said, it's important for all of us to recognize that humans and human behavior tend to represent the weakest link and a common avenue of approach for attacks whether sophisticated or rudimentary, whether targeted or commoditized in nature. While Providers and Sponsors with mature programs help to address this reality through measures including mandatory training and education, social engineering penetration testing and coaching, email and website filtering, or technical detection of potentially malicious links and attachments in email messages-- individual Participants in their daily lives can be more susceptible to such measures. Therefore, to help combat the external threat in the context of consumer actions, Sponsors and Providers must continue to develop and provide secure, encapsulated means for Participant interaction. The order of the day is to protect the data, protect the application, and protect the session to safeguard Participants in their interactions with the plan, as opposed to protecting the public end user computing environment altogether. Reducing the dependencies upon the consumer's endpoint security while maximizing the dependencies on the factors we can control represents a thematic imperative for Providers and Sponsors in this regard.

- **TRUSTED INSIDER** risks are a second key category, and they represent the intersection of where human procedural controls compliment technical controls. What are dangerous combinations of access or internal activity that business leaders should be concerned about from the Participant perspective? How could internal control considerations like this, if inadequately considered, be used by a deliberate or inadvertent insider to the detriment of Participants? How might an external actor potentially compromise a trusted insider who maintains such dangerous combinations of access? Essentially, this question goes beyond effective end user training and monitoring. It is not a discrete question of trusting or distrusting associates. It is incumbent upon Providers and Sponsors to introspectively identify and minimize such potential combinations from the business perspective as the basis of designing and maintaining reasonable segmentations of access, operational activity, and potential impact.

- The final high level threat category I'd like to note is important, and it centers around **THIRD PARTY** controls and monitoring. As business process outsourcing and cloud provider options for Providers and Sponsors continue to grow, so grows the requirement to externally monitor and govern what were previously internal points of visibility. A couple of key points here- First, due diligence of each service provider is a recurring deliverable, not a one time, pre-contract consideration. Actively demonstrating leverage of "right to audit" clauses and maintaining an ongoing, operationalized control dialog with key providers is crucial. Second, I believe that due

diligence including prescription of and monitoring around key controls to protect operations and Participants' information must be done on an engagement by engagement basis-- not a vendor by vendor basis. The idea of an "approved vendor" is a dangerous one-- what are the specific activities and controls for the specific service a Sponsor or Provider is asking of that vendor? Isn't that answer different depending upon the engagement or activity? The answer is yes, and while conducting third party due diligence this way is resource intensive, it's the right thing to do. This of course also applies directly to the relationship between Sponsors and Providers. Providers should welcome such due diligence by the Sponsor, and the Participant should expect it of both.

At the Participant level, there exists an inherent challenge in that each Provider or Sponsor typically represents but one such online or mobile relationship with each consumer. However, just as we see no competitive advantage in security in general, we all benefit from raising the level of awareness and "healthy skepticism" among the collective user and participant base. It is not a gross oversimplification to state that Phishing and e-mail borne attack vectors represent the biggest common thread to how consumer level vulnerabilities are exploited. How sponsors and administrators facilitate online interaction with participants... and therefore how such expectations are solidified over time... can be one of the greatest ways to help in this space. As examples:

- The use of properly authenticated self-service portals to send and retrieve information with participants is good, as it "trains" the Participant that deviations from this model may represent less secure anomalies. We want consumers to be wary of non-standard interactions, and adhering to the concept "if you see something, say something", to contact the Sponsor or Provider directly through known, established channels if ever in doubt. Ad-hoc distribution of materials via e-mail or other out of band methods only continues a dangerous socialization among participants that an e-mail in their inbox attempting to social engineer them is possibly legitimate. The unfortunate fact is that many or most individuals across the population in general-- including the Participants we strive to protect-- will click on just about any plausible looking link or attachment presented to them. In all such endeavors across financial services, the imperative is to train and communicate... and then practice... that we will NOT ask for Participant credentials via e-mail... that we will NOT solicit information via this medium...if ever in doubt, go directly to the website and log in with your credentials, use the vendor provided application... or call the provider directly. As an extension of this I encourage the idea of adaptive "step-up" authentication, not only based upon the sensitivity or transactional nature of the activity, but also based upon frequency of Participant interaction, the form factor of the device they are using, etc.

- Some Sponsors prescribe a model of allowing their Participants to access the Provider only from the Sponsor's secured environment rather than directly from the consumer space. While there are consumer convenience factors each Sponsor considers here, I believe that this model delivers inherent security benefits for the Participant and reduces potential points of vulnerability, complexity, and opportunity for social engineering attackers.

A primary challenge is that Providers cannot manage the Participant endpoints, particularly when accessing individually from their own homes, computers, or personal devices as opposed to from within their plan sponsor's network environment. We also can not as directly "train" them as we do our internal associates including with methods like social engineering penetration testing and coaching content. I was just last week talking with a peer CISO of one of the largest retailers in the world who recounted how they see millions of consumer connections per day using antiquated operating systems including Windows 2000, antiquated browsers including IE6, which have not been supported for years and therefore are not and cannot be patched against common vulnerabilities and exploits. These situations are not disproportionally concentrated in emerging markets or geographies, many end users adhere to the "if it's not broken, don't fix it" mentality and don't upgrade personal operating systems, browsers, or endpoint anti-malware subscriptions beyond the support included with their original purchase of the hardware or device. These are logically many of the same population who are retirement plan Participants. This leads us to basics of how we secure the session, for instance, forcing or restricting what levels or versions of Secure Socket Layer (SSL) encryption our customer facing applications will negotiate with and support to allow a browser session. As an example, the widely reported Heartbleed vulnerability during Q3 2014 led most Enterprises and administrators to restrict or disable SSL version 3 for customer facing applications. This is an example of where providers can set parameters "forcing" a participant to use certain specific or minimum controls or protocols on their devices in order to log on and interact successfully. Setting minimum browser, operating system, java, etc. versions required for successful connection and interaction helps to "compel" consumers to maintain good computing hygiene. However, we must always balance this logically against operational risks of denial of service, and always allow alternative means of interaction including call centers, etc.

Thank you again for this opportunity to briefly outline some thoughts on the Cybersecurity environment we face, and to describe some key considerations for Providers, Sponsors, and Participants. I'd like to conclude where I began, with the recognition that our fiduciary responsibility to protect supported Sponsors and Participants is core to our business model, and represents a commitment at every level of our organization. With that, I'm happy to address any questions that the Committee may have.