Written Testimony of Alla Goldman Seiffert
Director of Cloud Policy and Counsel
Internet Association

Before the House of Representatives Committee on Financial Services
Task Force on Artificial Intelligence hearing:
"AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers"
October 18, 2019

Internet Association (IA) represents over 40 of the world's leading internet companies. We support policies that promote and enable internet innovation and are dedicated to advancing public policy solutions that strengthen and protect internet freedom, foster innovation and economic growth, and empower users.

Our companies are also global leaders in the drive to develop lower cost, more secure, scalable, elastic, efficient, resilient, and innovative cloud services to customers in both the private and public sectors. The major U.S.-based hyperscale cloud providers are all members of Internet Association.

To begin, I would like to give a brief overview of cloud computing. NIST defines cloud computing as a model for "enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1] Typically, cloud service providers (CSPs) make available to customers a wide range of services that function as information technology building blocks that customers can use to build applications to meet their IT goals and be more secure, innovative, and responsive to their customers. These services are standardized and made available to all customers, including financial institutions.

A key benefit of the cloud is that CSPs are responsible for managing and securing certain aspects of the IT infrastructure supporting the services that customers use. Security is a top priority for CSPs and they invest a tremendous amount to make all of their services secure. By using these services, customers such as financial institutions can focus on carrying out core business functions and benefit from the security measures that CSPs have in place, as well as use security services that CSPs have developed to further protect their environments. In particular, IA member CSPs invest billions in cybersecurity and deploy resources and people in ways that simply cannot be matched by any single institution alone.

[1] Special Publication 800-145, National Institute of Standards and Technology, U.S. Department of Commerce, *NIST Definition of Cloud Computing: Recommendations of the NIST,* Peter Mell, Timothy Grace, September 2011. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

It is important to note that customers are responsible for determining the type of data that they store in the cloud and the types of applications they choose to run in the cloud. Indeed, financial institutions remain accountable for managing the risk of their IT environments, whether run in-house, through a third party (e.g., a managed service provider), or with a CSP. Financial institutions use the cloud for a wide range of applications, from storing publicly available data or running test environments to create new digital channels, storing more sensitive records, and running more critical workloads. In each case, customers' implementation of cloud services begin with the default security configuration that CSPs put in place, and each can take further steps to design, reconfigure, and manage their IT risks within their risk tolerance. While cloud computing use in the financial services industry is still nascent, cloud's security, scalability, and resilience features allow firms of all sizes to better manage risk.

Today, my testimony will identify several benefits and opportunities that cloud adoption creates for financial services firms, and I will focus on three central themes:

A. First, **cloud implementation is a shared responsibility between CSPs and customers.**
B. Second, **cloud adoption increases cybersecurity.**
C. Third, **cloud increases the resilience of our nation's financial institutions.**

Cloud security is a shared responsibility

As financial services firms look to achieve greater operational efficiency and modernize existing systems, they are increasingly turning to CSPs to manage their infrastructure and computing needs. Financial institutions that use cloud computing operate in an environment where they manage certain aspects of their IT resources and are responsible for configuring their use of cloud resources, but they rely on the CSP to manage other portions of their IT resources. This division of labor means that both the CSP and the customer bear responsibility for making sure the services are run efficiently and securely. Because each party is responsible for securing the resources they control, security in the cloud is what we call a "shared responsibility."

In general, the shared responsibility model means that CSPs are responsible for making sure the services they offer are secure and reliable, and CSPs give customers the ability to configure those services to achieve their business outcomes, including configuring the security settings of the services that they utilize. Certain cloud capabilities like application management, network configuration, and encryption settings are also the responsibility of the customer.

Simply put, CSPs are responsible for the security **of** the cloud, while the customer is responsible for security of the resources they store and process **in** the cloud. CSPs provide a broad range of information, tools, and assistance to help customers understand and properly administer their responsibilities.

In practice, this means CSPs protect the underlying infrastructure of their cloud and data centers from vulnerabilities, intrusions, fraud, and abuse.[2] While the specifics of this can be rather technical, these details are essential to understanding the shared responsibility model. In order to provide secure cloud infrastructure, CSPs manage and control the host Operating System (OS), the virtualization layer, and the physical security of its facilities. Customers are responsible for securely configuring the environments and applications that they deploy in a cloud environment, and CSPs also provide their customers with necessary security capabilities that can be configured to meet customers' unique security needs.

To ensure security within a given cloud environment, the customer configures and manages the security controls for the guest OS and other applications (including updates and security patches), as well as for the security group firewall. Customers also have the ability to configure cryptographic protection for certain services, which can be important based on the type of data and usage of workloads in the cloud environment. In some cases, CSPs may encrypt all customer information by default.

There are different service models for cloud computing, and customers may have more, or fewer, security responsibilities, depending on the types of services they use.

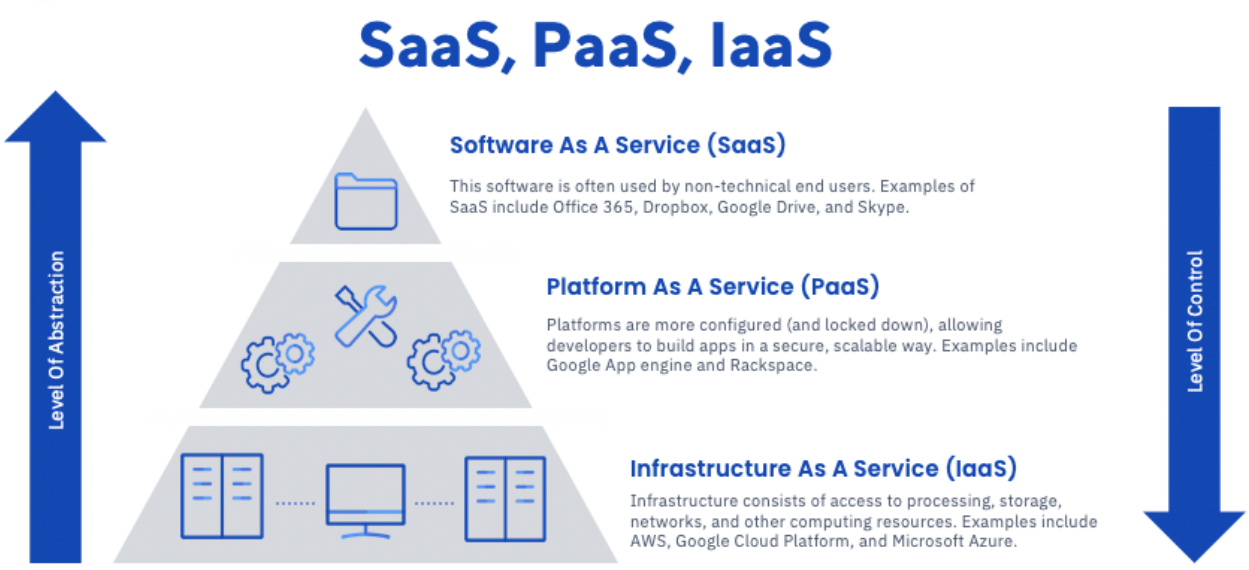

Figure 1: Diagram of IaaS, Paas, and SaaS as they relate to abstraction and level of end-user control.

It is important for financial institutions to have a clear understanding of the resources they are using when running in the cloud, and how the shared responsibility model applies to their applications. There exist domains of IT security controls that financial institutions should keep

[2] Panetta, Kasey. "Is the Cloud Secure?" Gartner. Gartner, Inc, October 10, 2019. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/.

in mind when using the cloud. CSPs manage those controls associated with their physical infrastructure and certain other aspects of their environment that may previously have been managed by the customer.

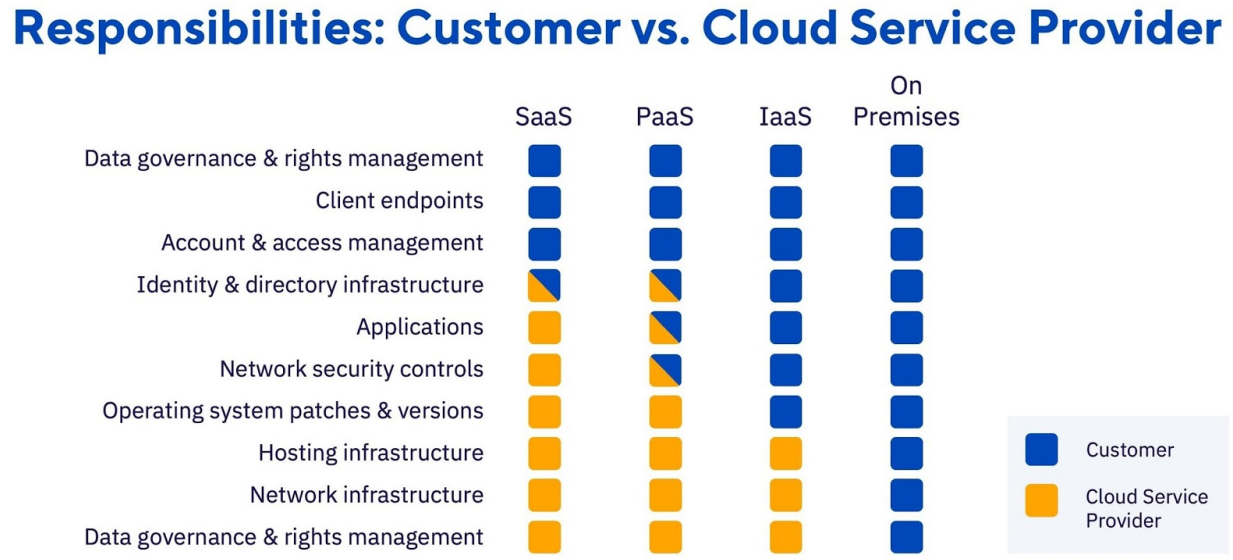

Figure 2: compared responsibilities between SaaS, PaaS, IaaS, and on-premises cloud models

In the financial services context, customers' security requirements will be informed by their own internal standards, as well as regulatory requirements and expectations.[3] The cloud model allows firms to implement best-in-class security controls and tailor them to the specific systems and workloads that each firm is running. Each customer is responsible for determining their security requirements and the cloud enables customers to meet those requirements. In addition, certain CSPs may offer tools, dashboards, and other real-time information and documentation to provide customers with information about configuration management, including how to configure services to meet appropriate requirements, such as implementation of multi-factor authentication or methods to enhance resiliency of services through data redundancy based on how the application is configured.

Even though CSPs are responsible for securing certain aspects of the cloud environment, customers are able and encouraged to evaluate the effectiveness of CSPs' security controls. CSPs provide assurance about the security of their environments through many mechanisms, including certifications from independent third-party auditors against industry standards. These audits speak to the design and implementation of CSPs' control environments. Customers then can use CSPs' control and compliance documentation available to them to perform their control evaluation and verification procedures as required by their internal

[3] II.C.20(a) Outsourced Cloud Computing, Federal Financial Institutions Examination Council (FFIEC), *IT Examination Handbook Infobase.* https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic20-oversight-of-third-party-service-providers/iic20(a)-outsourced-cloud-computing.aspx

compliance standards. Financial institutions typically incorporate the use of cloud into their risk management frameworks. Customers can use the assurance mechanisms that CSPs make available to ensure that they are adopting cloud in a manner consistent with their risk frameworks.

Cloud Increases Security Across Financial Services Firms

Cloud adoption helps banks increase overall security by modernizing applications and gaining better visibility into their networks, traffic, and vulnerabilities. The opportunities offered by cloud computing enable enterprises to significantly strengthen their IT security posture and implement best-in-class cybersecurity solutions.

Cloud application and infrastructure architects are presented with the opportunity to develop solutions that provide a business function while also designing systems securely. Financial institutions can leverage the security solutions implemented by CSPs to meet compliance and regulatory requirements to operate in a secure manner.

Financial services institutions are subject to regulatory and compliance requirements to ensure that their IT infrastructure is secure, to protect their and their customers' data, and ensure privacy. Financial services institutions are ultimately responsible for understanding these requirements and defining how they apply to their applications. This may include, for example, conducting due diligence and monitoring to ensure the security and resiliency of their CSPs' environments and taking steps to ensure that they architect their cloud environments in a secure, resilient, and compliant manner.

The cloud enables financial institutions to meet these security requirements and benefit from the operational efficiencies and other business opportunities that scalable technology has to offer.

The Department of the Treasury published a *Fintech Report* and put it thusly:

> The ongoing digital transformation of the financial services system is being driven not only by developments in computing power, the expanding ubiquity and interconnection of computers and mobile devices, and the exponential growth in digitized financial data, but also by technologies that can benefit from advances in data and computing capacity at greater scale and with greater efficiency. **Scalable technologies such as cloud computing enable financial services companies to store and process vast amounts of data and to quickly add new computing capacity to meet changing needs.** At the same time, advances in big data analytics, machine learning, and artificial intelligence

> are expanding the frontiers of financial services firms' abilities to glean new and valuable business insights from vast datasets.[4]

Large cloud service providers typically have the resources and expertise to invest in and maintain state-of-the-art and comprehensive IT security and deploy it on a global basis across their platforms. Financial institutions, especially small and mid-sized firms, could find it economically infeasible to achieve similar levels of security on their own. Moreover, because customers can rapidly redistribute data across a CSP's geographically diverse storage and processing centers, cloud environments can enhance firms' strategies for business continuity.

Increased Resilience

Another key benefit of using cloud computing is that the use of cloud services enables financial services firms to design applications to be more resilient. Cloud allows firms of all sizes to leverage a suite of best-in-class tools for backup, continuity of operations, and redundancy.

CSPs design their infrastructure to be resilient to outages and incidents, and customers can take advantage of this infrastructure to establish enhanced operational resilience. CSPs arhitect their global infrastructure to protect against physical disruptions and to make available redundant IT components to customers. For example, major CSPs' infrastructure consists of multiple data centers in locations all over the world. Within a single metropolitan region, some CSPs organize groups of data centers into an "Availability Zone" (AZ). AZs are physically separated and independent from each other and are built with highly redundant networking to withstand local disruption.

Customers are able to design applications so that they utilize multiple AZs within a single region. By implementing this type of design pattern, customers increase the resiliency of their applications. In the unlikely event an AZ fails, this architecture allows applications to continue running seamlessly using resources in the other AZs. This protects customers, while allowing core business functions to continue uninterrupted. Customers are also able to keep redundant copies of data in both multiple AZs and multiple regions to ensure broader availability and durability.

Customers are further able to apply this design pattern to achieve even greater operational resilience by architecting applications to make use of more than one region. Cloud-specific features, such as regional autonomy, allow systems to operate freely in a region without dependencies on other regions. Cloud adoption can also facilitate system transparency and insights necessary to make automated decisions.

---

[4] U.S. Department of Treasury, *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation,* Steven T. Mnuchin, July 2018. https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf

Financial services institutions are responsible for identifying their resiliency requirements, but the cloud enables them to build particularly resilient applications in line with broader risk management goals. For instance, by embracing key features of cloud technology, firms can deploy Enterprise Business Continuity Management (EBCM) across their entire technology stack. This is a risk and continuity of operations framework that enables companies of all sizes to think through (and plan) for a variety of scenarios that may befall the business. Cloud services play an integral role in provisioning extensible, flexible solutions that companies can configure to take advantage of seamless backup and restore services.

Conclusion

In conclusion, I would like to reiterate IA's gratitude for being included in discussions with the Committee Task Force on Artificial Intelligence and for the opportunity to testify here today. The IT postures of financial services firms have evolved a great deal over the years, and the internet industry is looking forward to supporting their continued growth and maturity.

Cloud computing has the power to meaningfully help financial services firms increase cybersecurity and resilience while also allowing firms to implement a shared responsibility model in managing their networks and data. IA – along with our members – stands ready to support the Task Force and Committee in helping financial services companies adopt cloud in a responsible way.

Thank you.