ECKERT SEAMANS ATTORNEYS AT LAW

February 23, 2023

Cybersecurity, Data Protection & Privacy Update

U.S. Department of Treasury Reports Highlights Pitfalls of Using Cloud Platforms

By Elizabeth Wilson and Matthew H. Meade

TREASURY SETS UP NEW INTERAGENCY CLOUD SERVICES STEERING COMMITTEE

*Critical Points **In a Nutshell***

- **What Happened**: The U.S. Department of the Treasury ("Treasury") released a report highlighting potential benefits and risks with the use of cloud in the financial industry and has set up a new interagency cloud steering committee to address these concerns.
- **Who Does This Affect**: U.S. financial institutions ("Institutions") who use cloud service providers ("CSP").
- **How This Affects You**: While the report itself does not impose any new requirements on financial institutions, regulators may use the report's findings to adopt new cloud guidelines.
- **Actions For You to Consider**: Institutions who use cloud services may consider:

  Applying a risk-based approach to its cloud design and implementation strategy, considering its regulatory environment, risk tolerance level, the particular services being requested, and how its cloud services are being used and configured;

  Ensuring its IT staff has specialized cloud expertise;

  Incorporating cloud scenarios when creating incident response and business continuity plans;

  Working with your CSP to design a resilient and user-friendly cloud solution that will decrease risk of system vulnerability and potential user misconfiguration; and

  Addressing transparency, risk management, and regulatory requirements in CSP contracts.

Additional Perspectives

On February 8, 2023, the Treasury released a report ("Cloud Report") highlighting the benefits and challenges of using cloud-based technologies in the financial industry and proposing actions to address these concerns. The Cloud Report is the result of the collaboration between the Treasury and the Financial and Banking Information Infrastructure Committee as well as input from other U.S. regulators and private sector stakeholders. The Cloud Report added a disclaimer stating that the Cloud Report does not impose any new requirements on Institutions and "neither endorses nor discourages cloud service adoption by the [financial] sector" (Cloud Report, p. 62).

The Cloud Report identified six challenges for Institutions using cloud-based services, which are highlighted in the below table.

Challenge	Select Highlights from the Cloud Report
Insufficient Transparency to Support Due Diligence and Monitoring by Institutions (Cloud Report, pp. 49-50)	▪ Institutions struggle with obtaining adequate information from CSPs to support its risk management requirements. ▪ CSPs struggle with facilitating Institution requests for one-on-one in-person audits due to issues with scalability and maintaining the security of its multi-tenant platform.
Gaps in Human Capital and Tools to Securely Deploy Cloud Services (Cloud Report, pp. 50-53)	▪ Institutions face issues when conducting its IT support and maintenance responsibilities due to shortages of IT staff with cloud expertise. ▪ A lack of user-friendly cloud tools to easily configure and maintain the cloud environment can cause misconfigurations, which may increase the risk of data breaches.
Exposure to Potential Operational Incidents, Including Those Originating at a Cloud Service Provider (Cloud Report, pp. 53-57)	▪ Design choices for an Institution's cloud service offering may increase resilience to operational incidents, if practical challenges arising from such choices can be addressed.
Potential Impact of Market Concentration in Cloud Service Offerings on the Sector's Resilience (Cloud Report, pp. 57-59)	▪ Market concentration in the cloud services industry may result in one CSP security incident or service interruption impacting multiple Institutions at one time.
Dynamics in Contract Negotiations Given Market Concentration (Cloud Report, pp. 59-60)	▪ Institutions expressed difficulty incorporating necessary provisions in CSP contracts, however, this has been improving as CSPs are learning the unique needs of the financial industry.
International Landscape and Regulatory Fragmentation (Cloud Report, pp. 60-61)	▪ Institutions subject to foreign laws and regulatory authorities may need to adopt a hybrid cloud strategy due to cloud restrictions in certain jurisdictions. ▪ Some foreign regulatory requirements being imposed on CSPs may create a positive impact on the U.S. financial industry by increasing the resilience of cloud services generally being offered to Institutions.

Proposed Next Steps by the Treasury

The Treasury has stated in the report that it will engage with other U.S. and foreign financial regulators, cloud service providers and the financial sector to address the above challenges. The Treasury has identified the following actions to support its cloud strategy:

- Establish an interagency Cloud Services Steering Group to coordinate on cloud issues;
- Conduct tabletop exercises that will involve cloud service providers and Institution stakeholders;

- Develop approaches to increase coordination, collaboration, and information sharing with other agencies and Institutions regarding potential cloud risks;
- Create industry wide definitions and terms;
- Measure the concentration of "critical uses of cloud services" across the industry;
- Review incident response processes to improve communication among regulators, CSPs, and Institutions;
- Develop enhanced regulatory guidance on cloud risk management practices;
- Collaborate with foreign regulators on developing international "standards, principles and guidance" and improving bilateral relationships and communications with such foreign regulators; and
- Foster consensus on "cloud security controls, risk management practices and contractual requirements".

How We Can Help?

ECKERT SEAMANS ATTORNEYS AT LAW

This Cybersecurity, Data Protection & Privacy Alert is intended to keep readers current on developments in the law and is not intended to be legal advice. If you have any questions, please contact Elizabeth Wilson at 215.851.8497 or ewilson@eckertseamans.com, or Matthew Meade at 412.566.6983 or mmeade@eckertseamans.com, or any other attorney in our Cybersecurity, Data Protection & Privacy Practice Groups, or any other attorney at Eckert Seamans with whom you have been working for further information and assistance.