August 2024

FBIIC Agency Heads

Dear FBIIC Colleagues:

In July the U.S. Department of the Treasury and Financial Services Sector Coordinating Council (FSSCC) published documents under the joint Cloud Executive Steering Group (CESG) construct intended to provide financial institutions of all sizes with the most effective practices for secure cloud adoption. We would like to take this opportunity to thank our regulatory colleagues for the work you and your staff have provided in support of the CESG over the last year. We deeply appreciate the time and expertise you have contributed at all levels to these efforts.

When Treasury and FSSCC set out to address the gaps identified in Treasury's report on the Financial Services Sector's Adoption of Cloud Services through the CESG construct, our public and private sector co-chairs also determined that the completed work should provide more than a roadmap for financial institutions.

Treasury and FSSCC note that the Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), and Consumer Financial Protection Bureau (CFPB) have authority to examine the performance of third-party service providers for their supervised financial institutions. These agencies have jointly issued guidance regarding relationships with service providers to promote consistency in supervisory approaches and offer views on principles that support a risk-based approach to third-party risk management that financial institutions may consider when developing and implementing risk management practices for all stages in the life cycle of third-party relationships. Further, the FRB, FDIC, and OCC have promulgated regulations imposing requirements directly on bank service providers related to mandatory notifications in the event of cybersecurity incidents.

However, after collaborating for the last year to help close the gaps outlined in the Treasury Cloud Report, the FSSCC and Treasury have concluded there is still a need for broader regulatory requirements to provide assurance on the security and resiliency of cloud services utilized by financial institutions. This letter to our regulatory counterparts outlines the actions we have taken to date and includes areas where Treasury and FSSCC believe that additional regulatory assistance incorporating key aspects of these deliverables would greatly benefit the continued security and resilience of the financial services sector:

- **Cloud Lexicon:** The CESG Cloud Lexicon is a foundational document that captures the most prominent terms used by cloud service providers (CSPs) and financial services sector cloud users for a single repository and reference point. The Cloud Lexicon will support the ability of CSPs and financial services sector institutions of all sizes to speak in standardized terms when negotiating contract terms, establishing security schema, and adhering to regulatory requirements. The document defines over 100 terms, is based on a

review of more than 20 industry standards and governmental resources, and includes input and review from financial institutions, regulators, and CSPs.

Recommendation: We recommend the financial regulatory agencies leverage the Cloud Lexicon as a baseline reference document in the supervision and examination of financial institutions and their CSPs.

- **Cloud Profile 2.0:** The Cloud Profile 2.0 is an extension of the Cybersecurity Profile created by the Cyber Risk Institute (CRI), which is a tool based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework and is intended to serve as a cloud security implementation plan for financial institutions of all sizes and functions. It provides a framework for both financial institutions and CSPs and will serve as a common tool developed by the financial sector and CSPs to assist financial institutions in ensuring secure cloud implementation, while allowing the document to evolve as standards change over time.

  Recommendations: We encourage the Federal Financial Institutions Examination Council (FFIEC) to issue a public statement emphasizing the benefits of using a standardized approach to assess and improve cloud security through the use of risk assessment tools like the Cloud Profile 2.0 and other pertinent frameworks or standards to self-assess and convey the specifics of each of their own cloud security programs to regulatory authorities, similar to the FFIEC 2019 Profile press release acknowledging the Cybersecurity Profile.

  Additionally, we request the FFIEC incorporate and reference the Cloud Profile 2.0 and other acceptable practices for sound cybersecurity into FFIEC IT handbooks and other pertinent guidance similar to the reference to the Cloud Security Alliance in the FFIEC IT Examination Handbook, "Architecture, Infrastructure, and Operations."

  The FSSCC and CRI have already provided and stand ready to continue to provide to examiners overview briefings, training, and webinars at annual examiner training conferences to assist in familiarity with the Cloud Profile 2.0 as a useful tool for financial institutions. We recommend that the FFIEC continue to incorporate the Cloud Profile 2.0 and other acceptable practices for sound cybersecurity into annual examiner awareness and training events, to familiarize examiners with the product. This could also include reference to the Cloud Profile 2.0 in communications such as the OCC's Cybersecurity Supervision Work Program referencing the Cloud Profile 2.0 or the FDIC and state banking agency InTREX program.

- **Transparency and Monitoring for Better "Security-by-Design":** This document is composed of two outputs for financial institutions with workloads running in CSP environments. The first is a service inter-dependency and resilience model that is a combination of service transparency, architecture best practices, and more detailed information about how a CSP manages the resiliency of its own major services. The second proposes baseline security outcomes expected in financial institutions' deployment of workloads running in CSP environments ("security by design" and "one-click" security) that make it easy for financial institutions to quickly turn on secure infrastructure with minimal engineering. These are resources that financial institutions of all sizes can use today to enhance their resiliency and provides CSPs clear outcomes that would help financial institutions meet their industry and regulatory expectations.

Recommendation: We encourage all financial sector stakeholders to continue conversations on the concepts of resiliency, transparency, and secure by design detailed in the Transparency and Monitoring "Secure by Design" document and promote the document's use as a resource for regulated entities.

- **Financial Sector Cloud Outsourcing Issues and Considerations:** This document identifies a non-exhaustive list of key considerations for developing contractual language between financial institutions and CSPs to address risks, regulatory requirements, and supervisory expectations when using cloud services. These key considerations may be used as a voluntary reference tool by financial institutions during the contract negotiation phase of onboarding a CSP to appropriately address cybersecurity, resilience, and third-party due diligence expectations, and to enable compliance with growing financial services regulatory requirements and supervisory expectations.

  Recommendation: Given limitations in what financial institutions (especially small and medium-sized firms) can negotiate through individual private contracts with their CSPs, we encourage the federal financial regulatory agencies that examine CSPs under the Bank Service Company Act (BSCA) to include relevant information about CSPs' adherence to supervisory expectations in the examination reports that the agencies provide upon request to banks with active contractual CSP relationships. We ask that the appropriate regulatory agencies with BSCA authorities be resourced and supported to cover the primary CSPs engaged by the financial services sector. The FSSCC will, in turn, encourage financial institutions to leverage their primary regulator's assessment of any CSP with which they have an active contractual relationship. In addition, we encourage the financial regulatory agencies to harmonize requirements with foreign regulators.

We thank you again for your collaboration and diligent efforts to address these complex issues and provide meaningful solutions for the financial services sector and the American people. In light of how successful this effort has been, we look forward to future public-private partnerships and toward building and refining the model established by the CESG.

Sincerely,

Todd Conklin, Deputy Assistant Secretary for Cybersecurity and Critical Infrastructure Protection
United States Department of the Treasury

Deborah Guild, Chair
Financial Services Sector Coordinating Council