# Randal K Quarles: Brief thoughts on the financial regulatory system and cybersecurity

Speech by Mr Randal K Quarles, Vice Chairman for Supervision of the Board of Governors of the Federal Reserve System, at the Financial Services Roundtable 2018 Spring Conference, Washington DC, 26 February 2018.

* * *

Thank you very much for having me here at the Financial Services Roundtable's spring meeting. I am pleased to speak with you all about our financial regulatory system: both the broad principles that have been directing my approach to evaluating the regulatory system, as well as cybersecurity, which is a topic of great import to financial system participants and their regulators.

## Efficiency, Transparency, and Simplicity of Regulation

As I have said before, we have an opportunity to improve the efficiency, transparency, and simplicity of regulation. We have spent the past decade building out and standing up the post-crisis regulatory regime, and as a result we have made critical gains. The financial system is undoubtedly stronger and safer. We have robust capital and liquidity levels, an effective stress testing regime, and improved resolvability of our largest firms.

But at the same time, it is our responsibility to ensure that those rules are effective. And if we identify rules that are not working as intended, we should make the necessary changes. With the benefit of hindsight and with the bulk of our work behind us, now is a natural and expected time to evaluate the effectiveness of that regime.

Our efforts toward implementing those principles are underway. Federal Reserve Board staff members continue the review that I have previously outlined. The goal is to consider the effect of past regulatory initiatives on the resiliency of our financial system, on credit availability and economic growth, and more broadly, their costs and benefits. I am confident that that review will reveal some clear ways that we can improve the core post-crisis reforms.

## Cybersecurity

Let me now turn from regulation to supervision, and more specifically, to the topic of cybersecurity, which continues to be a high priority for the Federal Reserve. The Federal Reserve is committed to strategies that will result in measureable enhancements to the cyber resiliency of the financial sector. Given the dynamic and highly sophisticated nature of cyber risks, collaboration between the public sector and private sector toward identifying and managing these risks is imperative. While we know that successful cyber attacks are often connected to poor basic information technology hygiene, and firms must continue to devote resources to these basics, we also know that attackers always work to be a step ahead, and we need to prepare for cyber events.

Many of you provide services that are critical to maintaining the functionality of the financial system. Those critical services should be highly resilient. But at the same time, some of the solutions in place to improve the resiliency of those critical services may actually contribute to a cyber event. One example would be the replication of bad data across data centers. As the Federal Reserve thinks about its financial stability mandate, this concern will be a particular focus. Solutions will not come easily, but I am confident that with strong public and private efforts, solutions will emerge.

The Federal Reserve also focuses on the sharing of threat information and collaborates with a

number of partners toward protective mechanisms. We work with other domestic agencies as well as international authorities, and we have partnerships between the public and private sectors to introduce and participate in programs that combat the increasingly frequent and sophisticated cyber threats.

Specifically, we collaborate with government and industry partners to plan and execute cybersecurity tabletop exercises focused on identifying areas where sector resilience and information sharing can be enhanced. We also participate in community and industry outreach forums and actively share threat intelligence with sector partners including the Financial Services Information Sharing and Analysis Center (FS-ISAC). And we encourage financial institutions to work collectively through arrangements such as FS-ISAC so that threat information can be shared promptly and effectively.

Collaboration among many stakeholders on cybersecurity is critical to progress. The Federal Reserve has been working with, and will continue to work with, other financial regulatory agencies on harmonizing cyber risk-management standards and regulatory expectations across the financial services sector.

Specifically, we are focused on aligning our expectations with existing best practices, such as the National Institute of Standards and Technology's Cybersecurity Framework, and identifying opportunities to further coordinate cyber risk supervisory activities for firms subject to the authority of multiple regulators. We support industry efforts to improve harmonization across the sector, which are complementary to achieving our regulatory safety and soundness goals.

## Conclusion

The Federal Reserve continues to work toward improving both post-crisis regulation and our approach to cybersecurity. I hope that my intention to lay out the broad principles guiding us as we move forward was helpful. And while many of the areas will require additional work and may not have fast results, the Federal Reserve is committed to getting it right, and I look forward to those efforts.