Remarks by

Thomas J. Curry
Comptroller of the Currency

At the

Bank Information Technology Training Conference

Atlanta

October 2, 2012

Good morning everyone. Thank you, Carolyn, for your gracious introduction, and thank you, Aida, for inviting me to join you here in Atlanta today for the 2013 Bank Information Technology Training Conference. Each of you plays a critical role in supervising and examining how banks and thrifts use and deploy information technology.

The nearly 2,000 banks and thrifts we supervise range from community-based banks and thrifts with less than $250 million in assets to complex, global financial institutions that have assets of more than $1 trillion. But regardless of size, the safety and soundness of these entities depends on the quality of their enterprise risk management, and in this information-driven marketplace, that includes ensuring the security of the technology and data that today are as vital as any aspect of the business.

Operational Risk is an area of significant concern to me—in fact it was the subject of my first speech as Comptroller. For our purposes, let's define it as the risk of loss due to failures of people, processes, systems, and external events.

Operational risk is embedded in every line of business and every activity at a financial institution, and effective management of that risk is not optional for banks and thrifts, large or small. The good news is that while operational risk is high and rising, banks and thrifts can manage it, provided they identify, measure, mitigate, monitor, and report it effectively. That means that in addition to overseeing the traditional sources of risk—underwriting, securities, mortgages, and credit cards—we must also ensure that banks' information and information systems are secure, complete, and accurate for all their lines of business, no matter what the circumstances.

We live in rapidly changing times—the pace of advances in technology is breathtaking, and it has changed the way we live. As smart phones, tablets, and wireless Internet become ubiquitous, they are changing the business model of modern banking. Many customers do much or all of their banking without ever setting foot in a bank, while behind the scenes, banks and thrifts are moving important segments of their business to the so-called "cloud," often using a third-party servicer to handle data.

As Comptroller, I depend on my mobile phone and the Internet as much as anyone. The technology is amazing —so much so, that perhaps we are beginning to take it for granted as a modern convenience. But we must not forget that the same gadgets and supporting networks that make our lives easier also carry enormous operational, reputational, and other risks for banks and thrifts. The challenge we face is making sure banks effectively manage the risks these tools introduce while allowing them to take advantage of the advances in productivity and customer convenience they can provide. Above all, we must ensure that banks remain aware of, and mitigate the risks of data breaches or other equally serious threats.

Banks and thrifts are accustomed to incorporating technical advances into their businesses, and while most are vigilant and well-prepared, the financial sector remains a vulnerable target, subject to an ever-increasing level and sophistication of external threats. The source and motivation of such threats vary, ranging from phishers and hackers, out for money or notoriety, to terrorists and hostile nations bent on sabotage or worse. If nothing else, the chaos of 9/11 taught us that the financial industry needed a well-thought-out strategy for coping with disasters and strengthening the resilience of the system.

As part of the Financial and Banking Information Infrastructure Committee, the OCC is constantly helping to revisit and revise strategies to address the pressing needs that may follow a disaster. The government has designated banks and thrifts as Critical Infrastructure, meaning they are considered essential to a functioning society and economy. To consider ourselves prepared for the worst, it is essential that our banks and savings associations can remain operable in the event of a terrorist attack or natural disaster, and that they all have robust business continuity plans in place. So far, the news has been good—thanks to the efforts of many in both the private and public sector. But we must ensure that banks and thrifts remain vigilant.

In September 2008, we experienced a different kind of crisis, the financial chaos that followed the housing bust and badly damaged many banks and thrifts, leading to the failures of some of the most familiar names in the industry. Four years later, the financial industry is still sorting out the consequences of the financial crisis, and supervisory agencies are still working to craft an effective response to avoid a recurrence. We have begun to incorporate regulatory and legislative changes, such as the Dodd-Frank Act. Some of the Act's implementing rules have already been put into place; others are forthcoming.

Congress intended the increased reporting and oversight requirements of the Dodd-Frank Act to enhance the stability of the U.S. financial system overall. But due to their scope and breadth, these requirements also present significant challenges to the technology systems of banks and thrifts. Properly used, information technology can help offset some of that burden—for example, by improving how banks and thrifts collect, report, and analyze data. Taking advantage of these opportunities, however, will require major upgrades to IT infrastructures, and these changes, if not done the right way, have the potential to affect how these systems perform.

At the same time, as banks and thrifts continue their recovery from the financial crisis, they face increasing pressure on the bottom line. Given the costs related to ongoing security and regulatory compliance, some banks may seek to cut corners on information security systems and processes. This could be disastrous, and must be avoided.

The danger in cutting corners is clear: stretching systems and processes beyond their capacity will eventually cause them to break down, leaving sensitive information at risk, or rendering key operational and process controls ineffective. The mortgage foreclosure processing mess is just one example where failure to ensure adequate operational capacity has had real and severe effects on banks' profits, reputations, and most importantly, their customers. The banks and thrifts we supervise, small and large, must be vigilant in resisting this trend, and it is up to us to ensure that they are. They must invest wisely in their systems and processes, and where necessary, replace legacy systems. It is our job to make sure they understand just how vital it is to do this right.

A danger for banks and thrifts lurks in the reliability—or lack thereof—of third parties hired to manage data and provide IT knowhow, or even Internet access. It may come naturally to many bankers to assume that their information is being guarded as promised, but experience tells us breaches happen all too often. As supervisors, we need to encourage banks to secure information the same way they would bundles of cash—locked away in an impregnable digital vault.

Yet, as headlines attest, banks and thrifts have repeatedly found themselves the victims of lax security by third parties. Some security breaches at merchant processors have affected millions of credit card accounts. No matter who is at fault, customers look to the banks and thrifts that issued their cards to vent their frustrations. In addition to the costs of reissuing cards—and larger costs incurred for fraud and credit monitoring—the resulting damage to the reputations of banks and thrifts has been significant. This is not something we can ignore simply because it is difficult to quantify.

As supervisors, our foremost concern must be the safe and sound use of IT by banks and thrifts and their customers. Many of our banks and thrifts provide services internally, but increasingly, they are relying on Technology Service Providers, or TSPs. Some of you are on teams that examine these TSPs on an interagency basis, under the FFIEC umbrella. Regardless of the size or complexity of a particular TSP, as we make clear in our written guidance, whenever a bank or thrift enters into a third-party relationship, it must be mindful that while it can outsource the activity, it cannot absolve itself of the responsibility for the activity. Effective vendor management programs are not only a regulatory expectation; they are necessary components of effective enterprise risk management.

Supervising an area like IT, which is evolving even as I speak to you now, is one of our most challenging and complex missions. It demands individuals who — like you — have skill sets that go beyond your examination expertise and include a unique combination of management, leadership, and communication skills. These abilities allow you to serve as liaisons, and even interpreters, between bank management and other examiners, and between the OCC and other regulatory agencies.

You have demonstrated these talents many times over. You, the examiners at the OCC who specialize in bank information technology, have provided a great pool of talent for the agency over the years. Former BIT examiners now serve as large bank EICs, midsize bank

ADCs, and lead experts, among other positions. And of course, our Ombudsman, Larry Hattix, is a former BIT Specialist and district Lead IT Expert. I could go on because the list is long, but the point is that many BIT Specialists have moved to other areas of supervision or policy units, and they bring with them much-appreciated technical skills that help promote integrated supervision.

On behalf of the OCC, I applaud each of you for your ongoing contributions to the safe and sound operation of all the entities we supervise: community, midsize, and large banks and thrifts; federal branches; trust companies; and TSPs.

With all the new technologies available and the enhanced features of existing ones, this is an exciting time to be involved in supervising and examining the use of IT by financial institutions. All of you, as supervisors of the smallest community bank or thrift to the largest banks, have unique roles. You are counted on to be among the first to note trends and spot problems and, therefore, to help us in Washington develop the type of guidance that ensures these innovative products meet customer needs, protect customer privacy, and comply with laws and regulations.

Finally, I would like to commend you on your work for the OCC. We live in challenging times and no one knows that more than you, the examiners who serve as our eyes and ears and front-line defense. Thank you!

Now I look forward to responding to any questions you have for me.