Remarks by
Thomas J. Curry
Comptroller of the Currency
Before
RMA's Governance, Compliance, and Operational Risk Conference
Cambridge, Massachusetts
May 8, 2014

Let me begin by commending RMA and its leadership for organizing this conference, on this subject, this year, just as it has held them for the past seven. RMA is an organization that always seems to be out in front on the issues that matter most to financial organizations. Not coincidentally, they are also the issues that have been front and center for me as Comptroller.

In fact, I had only been in office a few weeks when I addressed the subject of operational risk and its growing importance as a safety and soundness challenge. I said at the time that addressing the challenges posed by operational risk would be among my foremost priorities as Comptroller. I signaled that the OCC would be looking for ways to ensure that the internal control processes of the banks we supervise are strengthened, so that the events that occurred in the years before, during, and immediately after the financial crisis don't happen again.

One such initiative—the OCC's proposed formal guidelines on heightened expectations for risk management, internal audit, and governance in large national banks—will soon come to fruition. In January we released proposed guidelines. The comment period closed at the end of March, and we are now evaluating the comments we received.

So let me spend a few minutes discussing our proposal—partly because I believe that the OCC's guidelines for heightened expectations for large banks hold real promise for improving the safety and soundness of the banking system, and partly because it is a subject in which RMA has taken such an active and constructive interest.

Even before the details of our proposal had been thoroughly parsed, one question was on many bankers' minds: "will these new heightened expectations apply to me?" This was an understandable reaction, especially from community bankers, who are especially sensitive to regulatory burden. And so, at a conference very much like this one just a few weeks ago, I reassured them that the proposal is focused only on large and complex institutions—a term defined in the proposal to mean insured national banks, Federal savings associations, and Federal branches of a foreign bank with average consolidated total assets of $50 billion or more. A bank with assets under that threshold might fall under the heightened expectations guidelines if and only if we determined that its operations were highly complex relative to its risk-management capabilities. We expect that this would occur only in the most extraordinary circumstances.

You may be wondering why we needed heightened expectations for institutions in the $50 billion-plus category in the first place. And you're almost certainly wondering what they will mean for you.

The answer to the first question—the "why"—can perhaps best be explained in terms of recent experience. One of the central lessons coming out of the financial crisis was that supervisory expectations for risk management, internal audit, and corporate governance in our largest and most complex banks needed to be substantially higher, especially for the most systemically important institutions. To achieve that goal, the OCC

began developing heightened expectations in 2009. In 2010, we discussed in detail with our large banks what would be expected of them. In 2011, we assessed their compliance. In 2012, we reviewed their remediation plans, evaluated the results and incorporated them into our risk assessments of the institutions.

We observed a wide range of corporate governance, audit and risk management practices among our portfolio of large banks during this period. This "field testing" of heightened expectations practices gave us a clear view of what were the best practices and minimum standards in this area. This maturation of heightened expectations practices and our on-the-ground experience led us to conclude that a more robust approach, providing for the possibility of an enforceable response, was warranted.

I expect that many of you are by now familiar with our proposed heightened expectations. There are two major components. The first component sets forth the minimum standards for the design and implementation of a bank's risk governance framework, which should be based on what the industry commonly refers to as "the three lines of defense"—front line units, independent risk management, and internal audit. The job of a risk governance framework and the three lines of defense is to ensure that the bank has an effective system to identify, measure, monitor, and control risk taking, and to ensure that the board of directors has sufficient information on the bank's risk profile and risk management practices to do <u>their</u> job, providing management with effective direction and advice.

This is where the second component of heightened expectations comes into play. It sets criteria for the board's composition and responsibilities, to ensure that boards have a minimum number of independent directors and that all board members have the

information, status, and authority to ensure effective oversight, including the ability to pose a credible challenge to management.

Some parties have expressed a preference for a less prescriptive way of achieving these goals. They would like to see more left to the discretion of each institution, reflecting the fact that different banks have different corporate cultures that require different approaches to risk management.

I understand these concerns and share them as a matter of principle. After all, the OCC has always taken pride in tailoring its supervision to the individual needs and circumstances of national banks and Federal savings institutions. That has not changed and it will not change.

I also want to assure you that we are giving serious consideration to the comments we received. When the guidelines are released in their finished form, I think they will reflect careful consideration of the comments.

However, I want to point out that many, if not all, of the specific requirements of our heightened expectations ask no more of our large, complex banks than they are—or should be—doing already. As one example—and I could easily cite others—the proposed guidelines require every covered institution to formulate an explicit, written statement of risk appetite. This, I recognize, is not as simple as it sounds. But determining how much and what kind of risk a large bank is prepared to take to achieve its corporate goals is a fundamental decision that these banks have to make. Once they make that decision, it is equally important that a large bank communicate its risk tolerance clearly throughout the organization, so that people up and down the ranks understand and conform to it. And

management must establish measurement and reporting systems so it can ensure activities stay within the stated tolerance.

Yet over the years we found instances in which large, complex, and highly interconnected banks allowed operational units to define risk appetite in terms of their own needs and priorities. At best, this resulted in organizational confusion. At worst, it contributed to major breakdowns in risk management. And for banks with such broad impact on the financial system and the economy, that is simply unacceptable.

One reason we feel it is so necessary to establish heightened expectations for risk management, internal audit, and governance capabilities at large institutions is that risk today, in an interconnected world, is qualitatively different—and far more difficult to manage—than it was even a few years ago.

When I look back to the beginning of my career as a bank supervisor—which I'd like to think wasn't all that long ago—I am struck by the issues that were not on our radar. Thirty years ago, the proposition that the risk associated with bank systems and processes would eclipse credit risk as a threat to safety and soundness would have been summarily dismissed. But here we are. It speaks volumes that some of the most significant losses banks have sustained in the last several years were attributable not to the loans they made but rather to lapses in operational risk management and the ensuing legal judgments, regulatory fines and reputational damage. Reported lapses in foreclosure processing, consumer lending practices, BSA/AML program weaknesses, trading activities oversight and reference rate manipulation are just a few high profile examples.

Furthermore, and most prominently of late, there has been an increase in the volume and sophistication of cyber-attacks. While banks have been effective in defending against direct attacks, they have nonetheless sustained large losses—both in dollars and in public confidence—as a result of successful attacks on interrelated third parties, such as major retailers. I've been heavily focused on this particular type of operational risk because of the pace at which it is increasing and because of its potential to undermine confidence in our institutions. I imagine that you and your organizations have been focusing more on it as well.

I should begin by acknowledging that this is hardly a problem unique to banking. Attacks on our information infrastructure are everywhere. No matter where hackers direct their attacks, no matter if their motive is politics, financial gain, or simple bravado, they undermine our collective sense of privacy and security.

For cyber criminals, banks are especially tempting targets—not only because banks are where the money is, but also because of the vast amount of proprietary information banks have about their customers. Some attackers target banks because they want to undermine confidence in our country's financial system. Penetrating the information defenses of any one system may enable attackers to penetrate another, and that in turn could enable more widespread attacks on the broader economy.

This is an area, however, in which it is particularly important to avoid hyperbole. Hackers have been around since the dawn of the Internet age. And while they have grown much more sophisticated, banks and their regulators have stepped up their game, too. Banks are applying more resources to bolstering their information security. I am struck by the increasing level of cooperation among banks to combat cyber threats and develop

effective risk mitigation tactics. That itself represents something of a cultural shift, as banks increasingly recognize that information sharing is not a competitive issue, but rather an essential component of a strategy to protect themselves and the entire financial sector.

Helping to make banks less vulnerable and more resilient to cyber-attacks has been one of my top priorities as Comptroller and as current chairman of the FFIEC. The FFIEC's Cybersecurity and Critical Infrastructure Working Group, formed at my initiative, is working with financial institutions and their critical service providers to effectively identify, assess, and mitigate cybersecurity risks. It is collaborating with law enforcement, intelligence, and homeland security agencies to improve the effectiveness of our supervision. Just yesterday, the FFIEC sponsored a cybersecurity webinar in which approximately 5,000 representatives of community institutions participated. Later this summer, we are piloting new examination procedures on cybersecurity. And of course, you've recently seen the FFIEC agencies working together to get pertinent information out to our institutions quickly, such as the joint alerts on the OpenSSL vulnerability, better known as the Heartbleed bug.

Nonetheless, all of us have more work to do. One area of ongoing concern is the increasing reliance on third parties. The OCC recognizes that third-party relationships can help banks achieve their strategic objectives. That said, third-party relationships warrant close attention, because poor performance on the part of service providers has the potential to do enormous damage to the banks that employ them. By way of illustration, one need only to think back to the role of mortgage servicing companies in the

foreclosure fiasco that ultimately cost banks billions of dollars in penalties and restitution and did incalculable damage to the industry's reputation.

The OCC has long considered bank oversight of third parties to be an important part of a bank's overall risk management capability. For that reason, we have issued a number of guidance statements that address the importance of managing third-party providers. This past October, we also updated our guidance on third-party risk management to emphasize the importance of overseeing critical activities throughout the lifecycle of the relationship.

As you may know, the OCC has authority under the Bank Service Company Act to regulate and examine bank service companies and to take enforcement action against vendors when they endanger the safety and soundness of the banks they do business with. There are some practical and statutory limits to this authority, which might best be viewed as a supplement to a bank's own program to identify, mitigate, and monitor third-party risks. But the OCC—often through the FFIEC—does examine service providers that support a large number of banks and that could, therefore, pose a risk to the financial system.

As it happens, increasing concentration among service providers is a major concern of ours, because it raises the possibility that a problem with a single large vendor could affect a large number of banks simultaneously. If third parties are not vigilant about risk management, their own systems could provide a point of entry for attackers seeking access to the financial system. It goes without saying that we are carefully monitoring developments in the sector and we expect banks to do the same as part of their own risk management programs.

That brings me to my final point. Cybersecurity issues are different in degree but not in kind from the whole range of operational issues being addressed at this conference. We have come a long way in understanding and managing operational risks—for example, in developing metrics for strengthening controls and oversight and in quantifying the capital needed to protect against operational risk failures. However, to be managed properly, operational risk issues must be viewed in terms of their impact on the entire enterprise, not merely as—to use cybersecurity as an example—an IT issue. That requires a fully integrated and comprehensive approach to risk management—which is exactly what the OCC's heightened expectations are intended to achieve. I am sure we will have a stronger, more secure banking system as a result.

Thank you very much.