Remarks by

Thomas J. Curry
Comptroller of the Currency

Before a Meeting of
CES Government

Washington, DC
April 16, 2014

Good afternoon. It's a pleasure to finally be here with you. I had very much hoped to join the CES Government conference in January, but as you know, the weather was not cooperative, and my flight was grounded. So, I was delighted to have this second opportunity to address this group, and I was especially pleased that you had scheduled it for mid-April, nearly a month after the official onset of Spring, when we could be sure that winter would be well behind us.

Well, not quite. As you know, the season of Washington cherry blossoms was followed this week by a freeze and near record low temperatures. Well, at least that's one thing that we can't blame on the Heartbleed bug.

Before I start, I should tell you that some members of my staff raised an eyebrow when they heard I was going to be speaking during the Consumer Electronics Show, since I am generally not considered the most technically sophisticated person at the OCC when it comes to the latest electronic gadgets. In fact, some of them think I would probably be more at home with the technology in use when the OCC was founded—and that was during the Lincoln administration.

But while I'm not the world's foremost expert on the newest computer games, I can tell you that I am spending more and more of my time on IT issues in general and cybersecurity in particular. In fact, there are few issues more important to me—and to the Office of the Comptroller of the Currency—than shoring up the industry's defenses against cyberattacks.

It's an issue that I've also raised in my capacity as chairman of the Federal Financial Institutions Examination Council, or FFIEC, an interagency body that brings together all of the bank regulatory agencies. Last year, I worked with the other members of the Council to set up a Cybersecurity and Critical Infrastructure Working Group, and that group has already begun

meeting with intelligence, law enforcement, and homeland security officials. This working group will also consider how best to implement the President's Executive Order on Cybersecurity, as well as how to address recommendations of the Financial Stability Oversight Council.

Of course, the financial industry isn't the only sector at risk for cyberattacks. However, it is one of the most attractive targets for terrorists and criminals alike. It's tempting to criminal elements for very basic reasons that were fully explained by Willie Sutton who said he robbed banks "because that's where the money is." And it's attractive to terrorists because of the potential to inflict significant damage on our nation's economic security and way of life.

The fact is, we live in a world where consumers use their cellphones to deposit checks, pay bills over the Internet, and make purchases at the mall by swiping a credit card, and they're very sensitive to any suggestion that those systems might not be secure. Those consumers probably don't give much thought to what goes on behind the scenes with payment and settlement systems, or for that matter, the software that processes checking and savings accounts. Yet the impact of a cyberattack on those systems could be even more disruptive than a data leak at a large retail store. It's one thing to worry about whether someone is making charges on your credit card, as troubling as that might be. It's quite another to worry about whether the accounts that hold your life's savings are secure.

Today, the global nature of the Internet means hackers can target bank systems from almost anywhere. That includes countries with regimes that, at a minimum, act as criminal havens by turning a blind eye toward illicit activities, and at their worst, sponsor attacks. As a result, financial institutions today face cyber threats not only from insiders and individuals acting alone, but from global networks of well-organized nation-states, criminals, and so-called "hacktivists."

The system is also vulnerable because of the banking industry's significant reliance on technology and telecommunications, and more important, from the interconnections between these systems. Banks not only operate their own networks and leverage the Internet, they also rely on third parties to support their systems and business activities. Some of these third parties have connections to other institutions and servicers. And each new relationship and connection provides potential access points to all of the connected networks, thereby introducing new and different weaknesses into the system. Ultimately, these interconnected networks are vulnerable

to attacks that may affect multiple organizations at one time. Moreover, the ubiquitous nature of the Internet means that a large part of the systems used by banks and third parties ultimately rely on telecommunications and technology that are outside of their direct control.

Third-party relationships have been a significant area of concern for years, and not just in the area of cybersecurity. We've unfortunately found it necessary to take serious enforcement actions against some of our large institutions for problems brought on by poorly-managed third-party relationships, from debt collection companies to telemarketers.

I'm not trying to discourage the use of third-party vendors. They provide important services to both large and small banks, and community banks in particular often use outside contractors to leverage expertise and resources that they can't support internally. But we do expect the banks and thrifts we supervise to recognize that third-party relationships also pose significant risks, and any institution that supplements its own resources with outside providers needs to have risk management practices in place that are commensurate with that risk.

Managing these vendor relationships is especially important in the realm of IT systems and information security, particularly with respect to smaller banks and thrifts. The largest banks we supervise have hundreds of employees involved in defending against cyber attacks—and we have dedicated teams of examiners evaluating their management of these risks.

But as the big banks improve their defenses, it is very likely that hackers will turn their attention to community banks. These smaller institutions can provide a point of entry into larger networks, and they may have less sophisticated defenses than large banks. Many depend upon third-party providers for their IT services, including security. That's understandable, but they still have to be able to assure themselves that these service providers have adequate controls and solid processes in place to protect them and their customers. This can be particularly problematic for community banks and thrifts that may not have the resources or specialized expertise needed to identify and mitigate these vulnerabilities. As a result, we are particularly focused on controls and risk management practices employed by vendors that provide services to banks and thrifts. In this regard, I believe that the FFIEC working group I mentioned a few moments ago will help in the process of improving awareness across the financial system, particularly among community institutions, about the evolving nature of the cyber landscape.

Those of you who provide services to banks are probably aware that we examine a category of vendors designated as Technology Service Providers, or TSPs, and that we also have

authority under the Bank Service Company Act to issue enforcement actions when necessary. In December, we issued a formal order against one vendor, requiring it to take action to address deficiencies that prevented it from restoring services to banks promptly after Super Storm Sandy.

That episode illustrates one of the key areas of risk involving third parties that is on the rise: the extent to which service providers are consolidating and leaving financial institutions more dependent upon a single vendor. As a result, deficiencies at one vendor have the potential to affect a large number of banks simultaneously.

A second, and related, trend that concerns us is the increased reliance by banks on outside vendors, including foreign-based subcontractors, to support critical activities. The reliance on foreign vendors presents special problems. Banks need to consider the legal and regulatory implications of where their data is stored or transmitted, and make a determination as to whether geographic limitations are needed in their contracts.

Finally—and perhaps most importantly—we are concerned about the access third parties have to large amounts of sensitive bank or customer data. For an industry in which reputation means everything, a single data breach involving confidential customer information can be extremely costly. Banks are particularly vulnerable to events that erode trust, and once an institution's reputation is damaged, it can take years to repair.

All of these risks are manageable. But they must be managed. What concerns us is that risk management practices haven't always kept pace with the risks institutions take on. Some banks that historically have been regarded as well-managed have found themselves in trouble because they underestimated the risk in third-party relationships and didn't have the right controls in place. As a result, they faced credit losses, compliance problems, litigation exposure, and loss of reputation.

Recognizing the importance of managing third-party relationships, the OCC issued updated guidance last October that focuses on risk management practices for critical activities throughout the lifecycle of the third-party relationship. It also stresses the important role of the board of directors and management in overseeing these activities. We expect the board and management to ensure that appropriate risk management practices are in place, that clear accountability for day-to-day management of these relationships is established, and that independent reviews of these relationships will be conducted periodically.

It's also important for a bank to consider the vendor's risk management practices and controls. For example, does the third party have a sound security program and adequate physical security controls? Is there a documented and well-tested business continuity plan? And does the contractor have a process for reporting security incidents?

Likewise, banks have been asking us to do more in the area of supervising critical service providers. While we won't go into every provider, we will examine service providers that support a large number of banks and that could, therefore, pose a systemic risk to the financial sector. However, even if we do supervise a service provider, that does not alleviate a bank of its responsibility to understand and manage risks involved in their third-party relationships. Our supervision does not take the place of due diligence or ongoing monitoring commensurate with the level of risk and complexity of the arrangement

Clearly, we have much work to do as regulators to make sure the banks and thrifts we supervise are doing everything possible to protect themselves. It's crucial that financial institutions, at the board and senior management level, are aware and engaged, and that they understand the risks posed by these threats and the measures needed to address them. That's an area of emphasis in our supervision.

However, senior level engagement shouldn't stop at the walls of the bank. To deal with cybersecurity effectively, institutions both large and small need to communicate with each other, as well as with relevant government agencies. The financial services community has robust public-private sector partnerships, which can be leveraged even more for the benefit of the system.

For example, the Financial Services Information Sharing and Analysis Center or FS-ISAC, which is an information sharing non-profit organization run by financial institutions, includes the OCC and other public sector agencies as members. Additionally, the Financial Services Sector Coordinating Council, which was formed by the private sector after the 9-11 attacks, brings together private sector firms and trade associations across banking, financial markets, and insurance. These organizations meet regularly with the regulators to discuss emerging issues and best practices and to work cooperatively on ways to deal with critical infrastructure issues facing the financial sector.

Effective information sharing in the industry will help to increase awareness within individual institutions and across the industry. It will enable the sharing of best practices,

techniques and strategies, and collective responses to wide-scale events. It will also help banks focus resources on the most significant areas of concern.

The OCC stands ready to help in any way we can, not just with the institutions we supervise, but for the industry and the system as a whole. In an age of interconnected systems, we have to look beyond individual financial institutions to the range of vendors and customers that have access to some part of its infrastructure and systems.

Finally, the key message I'd like to leave with you today has to do with the importance of collaboration. This is not a problem that can be addressed by one agency alone or by any one institution acting on its own. It is a threat that we can deal with only if we work together in a collegial and collaborative way for the good of our country.

Thank you. I think we have some extra time, and I'd be happy to use it to respond to some of your questions.