ORAL STATEMENT

OF

VALERIE ABEND
SENIOR CRITICAL INFRASTRUCTURE OFFICER
OFFICE OF THE COMPTROLLER OF THE CURRENCY

BEFORE THE

COMMITTEE ON BANKING, HOUSING AND URBAN AFFAIRS

UNITED STATES SENATE

DECEMBER 10, 2014

Chairman Johnson, Ranking Member Crapo, and members of the Committee, I am pleased to be here today to discuss the important issue of cybersecurity and what the OCC and the Federal Financial Institutions Examination Council have been doing to address cyber threats and vulnerabilities. These efforts include information sharing for the benefit of the banking industry, regulatory community, and the financial system overall. But first, I would like to thank Chairman Johnson for his many years of leadership in the financial services arena, and wish him well in his future endeavors.

There are few issues more important to the OCC and to our country's economic and national security than the risks posed to financial institutions by cyber attacks. We live in a world of rapidly evolving technology in which consumers store information in the cloud, pay bills with their computers, and use their cell phones to make purchases at the mall. However, these conveniences have also introduced new vulnerabilities into the financial system, making it more difficult to protect financial institutions and customer information from cyber attacks.

As risks evolve, financial institutions must adapt. Our job as regulators is to ensure that the institutions we supervise do everything possible to identify and manage vulnerabilities to these cyber threats and their ability to respond. To meet that objective, the OCC's supervisory framework includes ongoing monitoring and information sharing with other regulators, government agencies, and banks regarding emerging threats and changes to the risk landscape. It also includes the development and continual refinement of standards and guidance that set forth our expectations as to how banks should safeguard their systems and their customers' information including at their third-party service providers.

To complement these efforts, we are committed to maintaining a cadre of highly trained IT examiners. While all OCC examiners receive training on information technology risk management, we also cultivate examiners with specialized skills and experience to focus on evolving information security and other technology risks in bank operations. Our examiners assess bank compliance with our supervisory expectations to ensure that they are appropriately managing risks, and when necessary, directing them to take corrective action.

Comptroller of the Currency Tom Curry chairs the FFIEC, and one of the Council's top priorities is to strengthen the resilience of regulated institutions to cyber attacks. Under the Comptroller's leadership, the FFIEC created the Cybersecurity and Critical Infrastructure Working Group. The working group helps the FFIEC members collaborate on cyber-related examination policy, training programs, coordination of responses to cybersecurity incidents, and information-sharing and awareness efforts.

The working group has been quite active since its inception. In addition to sponsoring awareness and training webinars, it has drafted statements advising financial institutions about a variety of specific threats and vulnerabilities, including the Heartbleed and Shellshock vulnerabilities, and attacks on automated teller machines. The FFIEC, on behalf of its members, also recommended that all institutions join the Financial Services Information Sharing and

Analysis Center, a public-private partnership, which provides information about current threats and vulnerabilities.

A major initiative of the working group was to pilot a cybersecurity examination work program at more than 500 community institutions. This Cybersecurity Assessment evaluated the operating environment for each institution, and assessed its overall level of preparedness. The results of the assessment will help FFIEC members make informed decisions about how they prioritize actions to enhance the effectiveness of cybersecurity-related supervisory programs, guidance, and examiner training. The results are summarized in a general observations document that provides observations and questions that bank boards of directors and CEOs should consider when assessing their cybersecurity preparedness.

The Comptroller has emphasized the importance of communication, collaboration, and cooperation in all aspects of our mission, but nowhere is communication and collaboration more important than in the realm of cybersecurity, where the threat transcends agency jurisdictions and industry boundaries. The OCC is an active member of several information sharing bodies. We also recognize the importance of maintaining relationships with law enforcement and intelligence communities to share information through open lines of communication. We use information sharing forums, relationships with government agencies, and information from our examinations to inform our supervision.

Finally, the recent breaches at large retailers highlight the need for improved cybersecurity for merchants. When breaches occur in merchant systems, we believe that merchants should contribute to efforts to make affected consumers whole so that banks, particularly community institutions, do not disproportionately shoulder the cost. Additionally, financial institutions share dependencies with other sectors, such as telecommunications and energy, and as such we support efforts to ensure commensurate standards for these important critical infrastructures.

In closing, we are committed to refining our supervisory processes and to participating in a range of information sharing forums to keep abreast of and respond to cyber threats. Combatting threats and protecting our economic security requires the government and industry to work together for the good of consumers, the industry, and the entire financial services sector.

Thank you. I would be happy to answer questions.