Richard F. Chambers
Certified Internal Auditor
Qualification in Internal Audit Leadership
Certified Government Auditing Professional
Certification in Control Self-Assessment
Certification in Risk Management Assurance
President and Chief Executive Officer

T: +1-407-937-1200
E-mail: richard.f.chambers@theiia.org

January 16, 2017

Office of the Comptroller of the Currency
Legislative and Regulatory Activities Division
400 7th Street, SW
Washington, DC 20219

Response emailed to: regs.comments@occ.treas.gov

RE: Enhanced Cyber Risk Management Standards
Docket ID OCC-2016-0016, RIN 1557-AE06

Dear Sir/Madam:

On behalf of the more than 65,000 U.S. members of The Institute of Internal Auditors (IIA), I am pleased to provide a response to the joint advance notice of proposed rulemaking, Enhanced Cyber Risk Management, issued by the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation.

The IIA has a longstanding position that the presence of an effective internal audit function makes an unequivocal statement about the way an organization's leadership views strong and effective risk management, internal control, and corporate governance. As a result, we believe that the internal audit function would be well-positioned to provide assurance under the areas being considered in the proposed standards, as demonstrated by high-performing internal audit functions in the financial industry that already incorporate cyber risk management assessments in their overall audit plans. One of the main functions of internal audit is the evaluation of the corporate and IT governance structures and practices within an organization, in conformance with "IIA Standard 2110 – Governance":

The internal audit activity must assess and make the appropriate recommendations to improve the organization's governance processed for:

- Making strategic and operational decisions.
- Overseeing risk management and controls.

Global Headquarters
1035 Greenwood Blvd, Suite 401
Lake Mary, FL 32746 USA
T: +1-407-937-1100
F: +1-407-937-1101
www.theiia.org

- Promoting appropriate ethics and values within the organization.
- Ensuring effective organizational performance management and accountability.
- Communicating risk and control information to appropriate areas of the organization.
- Coordinating the activities of, and communication information among, the board, external and internal auditors, other assurance providers, and management.

2110.A2 – The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.

The evaluation of effective governance includes the assessment of key components, such as leadership, organizational structure, policies, processes, risks, and controls as described in The IIA's Global Technology Audit Guide (GTAG), **"Auditing IT Governance,"** issued in July 2012 (copy attached).

Due to the dynamic nature of cyber risks, as well as the varied size and industry role of certain covered entities, any standards resulting from the new rulemaking should permit flexibility for developing frameworks that would allow allocation of resources to effectively address areas of higher risk (Question 2). In addition, as the enhanced cyber risk management standards will apply to key vendors to financial institutions, The IIA recommends consideration for a new type of generally accepted, service provider cyber risk management reporting, as this would greatly reduce the burden on these vendors of having multiple clients conduct individual assessments (Question 4).

The IIA supports the requirement that covered entities structure cyber risk management into the Three Lines of Defense model. The participation of business units, and risk management in the implementation of cyber risk initiatives, is critical because IT management must have a clear understanding of the organization's objectives, risk profile, business processes, and dependencies on third parties to develop and implement the necessary controls to address cyber risks.

Internal audit as the third line of defense can evaluate the effectiveness of risk management, internal controls, and corporate and IT governance, and provide advice to the board to better manage an organization's IT environment within its risk appetite and tolerance.

Conformance with the following IIA standards currently prepare an internal audit function to discharge the responsibilities described in the proposed standards (effectively monitor, measure, manage and report on cyber risk):

1110 – Organizational Independence
1111 – Direct Interaction with the Board
2000 – Managing the Internal Audit Activity
2130 – Control
2420 – Quality of Communications
2440 – Disseminating Results

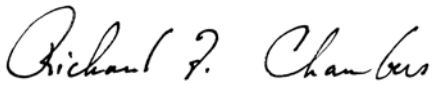
Reports on cyber risks, threats and vulnerabilities should include expert interpretation of the data so as to provide meaningful analysis for the board and executive management to make effective decisions. Internal audit can provide assurance reports on the effectiveness of the cyber risk framework, including vulnerabilities, and controls. However, mandating specific reporting frequency

may be inefficient, as the board and executive management should be kept informed, as necessary, when there is a significant weakness or cyber incident. The IIA recommends that the board and executive management work with internal audit to determine the nature of reports based on the current level of risk. Over time, the appropriateness of the report details can be reviewed and adjusted periodically by the board and executive management. (Question 15).

The IIA is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in New York in 1941, The IIA today serves more than 185,000 members from more than 170 countries and territories. The association's global headquarters are based in Lake Mary, Fla.

We appreciate the opportunity to provide our response to this joint advance notice of proposed rulemaking. If you have any questions about our response or would like to discuss further, please contact Kathy Anderson, The IIA's Managing Director of North American Advocacy. Ms. Anderson can be reached at Kathy.anderson@theiia.org or 1-407-937-1291.

Sincerely,



Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA
President & Chief Executive Officer

Attachment: Global Technology Audit Guide *"Auditing IT Governance"*

cc: Cassian Jae, Director, Financial Services Audit Center
Brad Jones, Director, Government Relations