

## ***Security Control Review of the Federal Reserve Bank of Richmond's Lotus Notes Systems Supporting the Board's Division of Banking Supervision and Regulation***

To evaluate the security controls and techniques of the information systems of the Board of Governors of the Federal Reserve System (Board), the Office of Inspector General reviews controls over Board applications on an ongoing basis. Consistent with the requirements of the Federal Information Security Management Act of 2002 (FISMA), we conducted a security control review of the Federal Reserve Bank of Richmond's (FRB Richmond's) Lotus Notes systems supporting the Board's Division of Banking Supervision and Regulation (BS&R). FRB Richmond's Lotus Notes systems are classified as third-party applications, and they are components of a general support system that is listed on the Board's FISMA application inventory under BS&R. The Lotus Notes systems are used by FRB Richmond to support supervision and examination activities.

Our audit objective was to evaluate the adequacy of selected security controls for protecting data in the Lotus Notes systems from unauthorized access, modification, destruction, or disclosure. To accomplish this objective, we used a control assessment review program based on the security controls defined in National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*. This document provides a baseline for managerial, operational, and technical security controls for organizations to use in protecting their information systems.

Overall, our review found that a number of actions have been taken to secure the Lotus Notes systems and that associated controls are adequately designed and implemented. However, we identified opportunities to strengthen information security controls to help ensure that sensitive bank supervision and examination information is protected and that the Lotus Notes systems meet FISMA requirements. In comments on our draft report, the Directors of BS&R and the Division of Information Technology generally agreed with our recommendations and outlined corrective actions already taken or underway. We will follow up on the implementation of these recommendations as part of our future FISMA-related audit activities. Given the sensitivity of information security review work, our reports in this area are generally restricted. Such is the case for this audit report.