Executive Summary:

Security Control Review of the Board's E^2 Solutions Travel Management System

2014-IT-B-012 **August 21, 2014**

Purpose

The Federal Information Security Management Act of 2002 (FISMA) requires the Office of Inspector General (OIG) to evaluate the effectiveness of the information security controls and techniques for a subset of the Board of Governors of the Federal Reserve System's (Board) information systems, including those provided or managed by another agency, a contractor, or another organization. As part of our work to fulfill this requirement, we reviewed the information system security controls for the Board's third-party E^2 Solutions Travel Management System (E2).

Our audit objective was to evaluate the adequacy of selected security controls for protecting Board data in E2 from unauthorized access, modification, destruction, or disclosure, as well as the system's compliance with FISMA and the information security policies, procedures, standards, and guidelines of the Board.

Background

E2 is a web-based travel management system that is used by multiple federal agencies to plan, authorize, arrange, process, and manage official travel. E2 has been the Board's official travel system since August 2010, and it is listed on the Board's FISMA inventory as a third-party application. E2 is classified as a moderate-risk system, and it contains sensitive financial and personally identifiable information on Board employees and contractors. The Division of Financial Management (DFM) is assigned overall responsibility for ensuring that the system meets FISMA requirements.

Findings

Overall, we found that DFM has taken several steps to ensure that security controls for E2 are implemented in accordance with the requirements of FISMA and the Board Information Security Program (BISP). However, we identified improvements that are needed to ensure that security controls in the areas of risk assessment, system and services acquisition, personnel security, and audit and accountability are implemented effectively and operating as intended.

Our report includes five recommendations that focus on strengthening risk management and contractor oversight processes to ensure that controls in these areas are implemented consistently with the requirements of FISMA and the BISP. In comments to our draft report, the Director of DFM concurred with our recommendations and outlined actions that have been or will be taken to address our recommendations. We believe that the actions outlined by the Director are responsive to our recommendations. We will follow up on the implementation of each recommendation in this report as part of our future audit activities related to the Board's continuing implementation of FISMA.

Given the sensitivity of information security review work, our reports in this area are generally restricted. Such is the case for this audit report.