GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-13-155, a report to congressional requesters

January 2013

INFORMATION SECURITY

Federal Communications Commission Needs to Strengthen Controls over Enhanced Secured Network Project

Why GAO Did This Study

In September 2011, FCC discovered that it had experienced a security breach on its computer network, which potentially allowed sensitive information to be compromised. The commission initiated the ESN project to implement enhanced security controls and an improved network architecture to defend against cyber attacks and reduce the risk of a successful future attack.

GAO was asked to assess the extent to which FCC has (1) effectively implemented appropriate information security controls for the initial components of the ESN project, and (2) implemented appropriate procedures to manage and oversee its ESN project.

To do so, GAO determined the effectiveness of ESN security controls by evaluating control configurations and identifying management controls; and determined how FCC applied them to the ESN project by analyzing documentation and interviewing commission officials.

What GAO Recommends

GAO is making seven recommendations to the FCC to implement management controls to help ensure that ESN meets its objective of securing FCC's systems and information. In commenting on a draft of this report, FCC concurred with the recommendations. In a separate report with limited distribution, GAO is also making 26 recommendations to resolve technical information security weaknesses related to access controls and configuration management of the ESN.

View GAO-13-155. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, Valerie Melvin at (202) 512-6304 or melvinv@gao.gov, and Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

The Federal Communications Commission (FCC) did not effectively implement appropriate information security controls in the initial components of the Enhanced Secured Network (ESN) project. Although FCC took steps to enhance its ability to control and monitor its network for security threats, weaknesses identified in the commission's deployment of components of the ESN project as of August 2012 resulted in unnecessary risk that sensitive information could be disclosed, modified, or obtained without authorization. This occurred, in part, because FCC did not fully implement key information security activities during the development and deployment of the initial components of the project. While FCC policy is to integrate security risk management into system life-cycle management activities, the commission instead deployed the initial components of the ESN project without, among other things, first selecting and documenting the security controls, assessing the controls, or authorizing the system to operate. As a result of these deficiencies, FCC's information remained at unnecessary risk of inadvertent or deliberate misuse, improper disclosure, or destruction. Further, addressing these deficiencies could require costly and time-consuming rework.

FCC's efforts to effectively manage the ESN project were hindered by its inconsistent implementation of procedures for estimating costs, developing and maintaining an integrated schedule, managing project risks, and conducting oversight. If not addressed, these weaknesses could pose challenges for the commission to achieve the project's goal of improved security. Specifically, FCC

- had not developed a reliable life cycle cost estimate for ESN that includes all implementation costs;
- did not, in its project schedule, adequately identify the sequence in which activities must occur, ensure that detailed activities were traceable to higher-level activities, or establish a baseline schedule;
- documented and managed some risks to project success, but its prime contractor did not identify any project risks until after the deployment of the initial components of the ESN project had begun; and
- had not included the ESN project in its processes for conducting regular oversight of information technology projects.

According to FCC officials, a key reason that they had not fully applied their policies or widely accepted best practices for security risk management and project management is because the ESN project was an emergency project and, therefore, needed to be initiated quickly. However, while GAO agrees that the security threat makes implementation urgent, it does not negate the need to perform key security risk management activities. Unless FCC more effectively implements its IT security policies and improves its project management practices and effectively applies them to the ESN project, unnecessary risk exists that the project may not succeed in its purpose of effectively protecting the commission's systems and information.