January 2003

GAO
Accountability • Integrity • Reliability

Highlights

Highlights of a high-risk area discussed later in this report (GAO-03-121)

HIGH-RISK SERIES

Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures

Why Area Is High Risk

Since GAO designated computer security in the federal government as high risk in 1997, evidence of pervasive weaknesses has been continuing. Also, related risks have been escalating, in part because of the dramatic increases in computer interconnectivity and increasing dependence on computers to support critical operations and infrastructures, such as power distribution, water supply, national defense, and emergency services. This year, GAO expanded this high risk area to include protecting the information systems that support our nation's critical infrastructures, referred to as cyber critical infrastructure protection or cyber CIP. Among other reasons for designating cyber CIP high risk is that terrorist groups and others have stated their intentions of attacking our critical infrastructures, and failing to protect these infrastructures could adversely affect our national security, economic security, and/or public health and safety.

What Remains to Be Done

Among other actions essential to sustaining federal information security improvements are the agencies' development of effective risk management programs and the development of a comprehensive strategy to guide agencies' efforts. Further actions to improve CIP include developing a national CIP strategy and improving analysis and warning capabilities and information sharing on threats and vulnerabilities.

www.gao.gov/cgi-bin/getrpt?GAO-03-121.

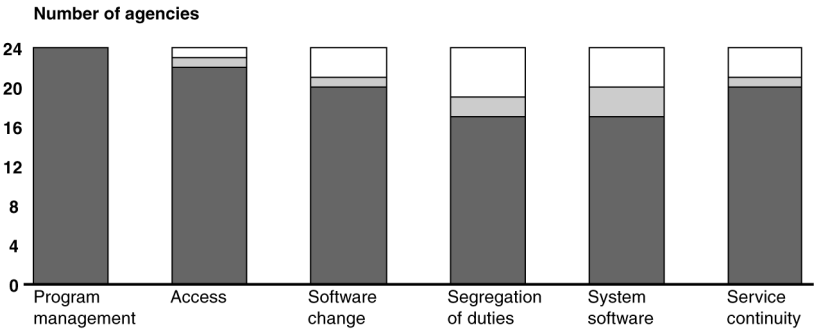
For additional information about this high-risk area, click on the link above or contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

What GAO Found

Since January 2001, efforts to improve federal information security have accelerated at individual agencies and at the governmentwide level. For example, implementation of Government Information Security Reform legislation (GISRA) enacted by the Congress in October 2000 was a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses. In implementing GISRA, agencies have noted benefits, including increased management attention to and accountability for information security. Although improvements are under way, recent audits of 24 of the largest federal agencies continue to identify significant information security weaknesses that put critical federal operations and assets in each of these agencies at risk (see figure below).

Over the years, various working groups have been formed, special reports written, federal policies issued, and organizations created to address the nation's critical infrastructure challenges. In 1998, the President issued Presidential Decision Directive 63 (PDD 63), which described a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. To accomplish its goals, PDD 63 designated and established organizations to provide central coordination and support. This directive has since been supplemented by Executive Order 13231, which established the President's Critical Infrastructure Protection Board and the President's *National Strategy for Homeland Security*. While the actions taken to date are major steps to more effectively protect our nation's critical infrastructures, GAO has made numerous recommendations over the last several years concerning CIP challenges. In response to these challenges, improvements have been made and efforts are in progress, but more work is needed to address them.

Information Security Weaknesses at 24 Major Agencies



Source: Audit reports issued October 2001 through October 2002.