GAO Highlights

Highlights of GAO-23-104705.

September 2023

CYBERSECURITY PROGRAM AUDIT GUIDE

Why GAO Did This Study

GAO has long recognized the importance of information security, initially identifying it as a government-wide high-risk area in 1997. Since then, the connectivity of systems has soared, and the sophistication of attacks has rapidly escalated.

Given the urgency to address the cybersecurity threat, GAO embarked on an effort to provide guidance to analysts and auditors on conducting cybersecurity audits. Such audits are essential to identifying cybersecurity program weaknesses and developing appropriate recommendations for agency corrective actions.

The development of the CPAG reflects GAO's collective experience over the last three decades in issuing hundreds of information security and cybersecurity audit reports and making thousands of recommendations. In developing the CPAG, GAO conducted extensive outreach with internal and external stakeholders. GAO also administered a questionnaire on existing guidance and received responses from 18 federal Office of Inspectors General, five public accounting firms, and four state audit offices.

In addition, GAO held 14 focus groups with internal and external stakeholders to discuss and review key cybersecurity practices. The focus group members comprised a cross section of federal, state, and local auditors and experts as well as private and non-profit sector officials. GAO also interviewed officials from the National Institute of Standards and Technology, the Center for Internet Security, and ISACA.

View GAO-23-104705. For more information, contact Nick Marinos at (202) 512-9342 or MarinosN@gao.gov, Vijay D'Souza at (202) 512-7650 or DsouzaV@gao.gov, or Jennifer R. Franks at (404) 679-1831 or FranksJ@gao.gov.

Why GAO Developed This Guide

The Cybersecurity Program Audit Guide (CPAG) is to be used in conducting cybersecurity performance audits. The intent of the guide is to arm cyber analysts and auditors with a set of methodologies, techniques, and audit procedures to evaluate components of agency cybersecurity programs and systems. GAO welcomes federal and other governmental organizations to use this guide to assess their cybersecurity programs.

The CPAG has six primary components:

The Cybersecurity Program Audit Guide's Six Primary Components

Source: GAO analysis of National Institute of Standards and Technology guidance; images: marinashevchenko/stock.adobe.com. | GAO-23-104705

- **Asset and risk management**: developing an understanding of the cyber risks to assets, systems, information, and operational capabilities.
- **Configuration management**: identifying and managing security features for system hardware and software and controlling changes to the configuration.
- **Identity and access management**: protecting computer resources from modification, loss, and disclosure by limiting authorized access.
- **Continuous monitoring and logging**: maintaining ongoing awareness of cybersecurity vulnerabilities and threats to an organization's systems.
- **Incident response**: taking action when security incidents occur.
- **Contingency planning and recovery**: developing contingency plans and executing successful restoration of capabilities.

Each of the above components has four to seven overall key practices. For each of these practices, the CPAG provides further specificity on control objectives, applicable criteria, and available audit procedures.

Although the CPAG provides suggested approaches for addressing key cybersecurity topics, it is intended to be used in a flexible manner. Depending on audit objectives and the relative importance of specific issues, organizations may adjust and fine tune audit techniques as appropriate.