

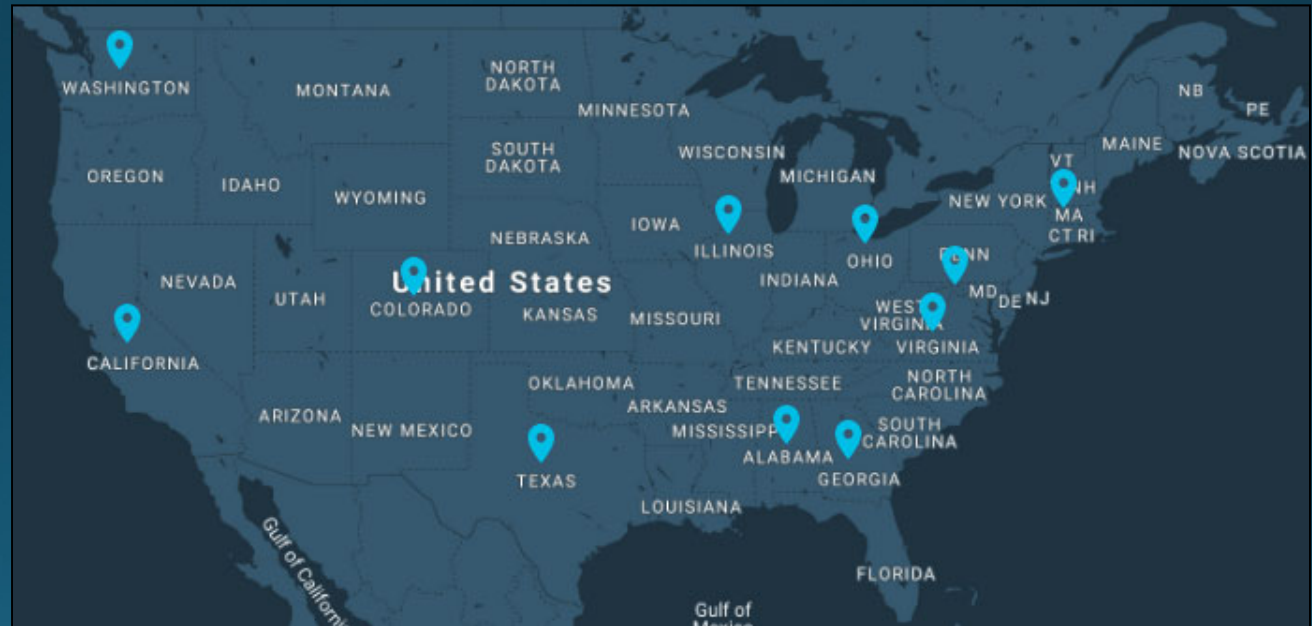
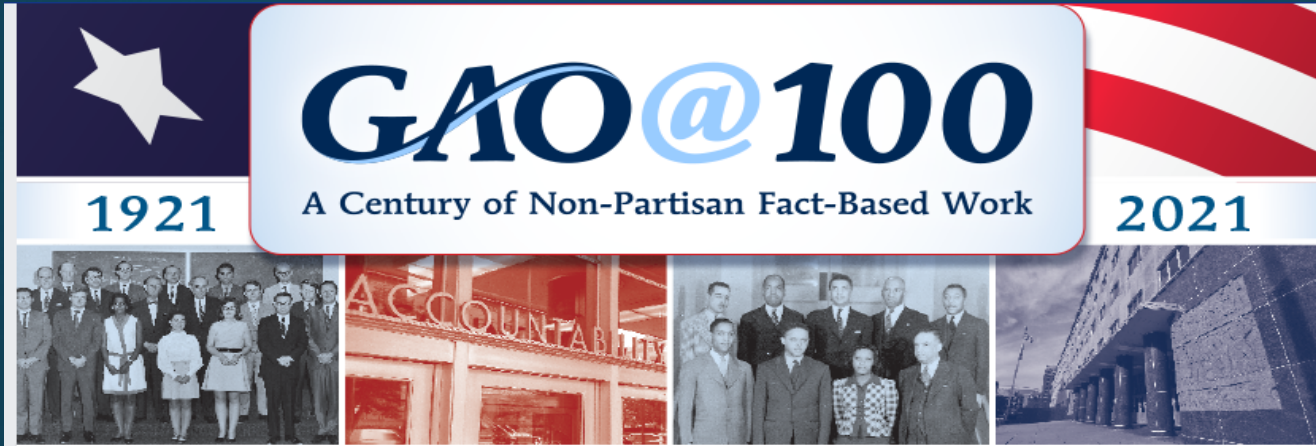
# **GAO's Methodology for Assessing Cybersecurity Controls**

**U.S. Government Accountability Office**

**December 2, 2021**

# Agenda

- About GAO
- Discussion of Federal Information System Controls Audit Manual (FISCAM)
- New Cybersecurity Audit Methodology Manual
- Next steps
- Q & A



Source: <https://www.gao.gov>

# GAO's Core Values

## MISSION VALUES:

### **Accountability**

Enhance the economy, efficiency, effectiveness, and credibility of the federal government

### **Integrity**

Conduct professional, objective, fact-based, non-partisan, non-ideological, fair, and balanced work

### **Reliability**

Produce timely, accurate, useful, clear, and candid products



## PEOPLE VALUES:

### **Valued**

Seek out and appreciate each person's perspectives

### **Respected**

Treat everyone with dignity

### **Treated Fairly**

Foster a work environment that provides opportunities for all



# Diversity, Equity, and Inclusion



# Fiscal Year 2021 Accomplishments

## By the Numbers: A look at our FY 2021 accomplishments



**\$66.2 billion**  
in financial benefits



**\$158 return**  
for each \$1 of our budget  
(5-year average)



**1,602**  
new recommendations



**over 1,200**  
improvements in federal  
government operations



**578**  
reports



**over 60**  
congressional  
testimonies



**about 2,000**  
bid protests  
handled



**over 500**  
legal decisions and  
opinions issued

# Recent GAO Blog Posts



## Challenges in Mapping the Digital Divide

OCTOBER 19, 2021

The divide between those who had access to broadband and those who did not was highlighted during...

## IRS's Efforts to Modernize 60-year-old Tax Processing System Is Almost a Decade Away

NOVEMBER 04, 2021

IRS relies extensively on information technology (IT) to process tax returns, collect taxes...

## Preventing Fraud in CARES Act Programs

NOVEMBER 16, 2021

Congress appropriated nearly \$5 trillion through the Coronavirus Aid, Relief, and Economic Security...



# Cybersecurity Work



Source: GAO File Photo.

Critical Infrastructure Protection:  
Education Should Take Additional  
Steps to Help Protect K-12 Schools  
from Cyber Threats. GAO-21-477  
Published: May 20, 2021.

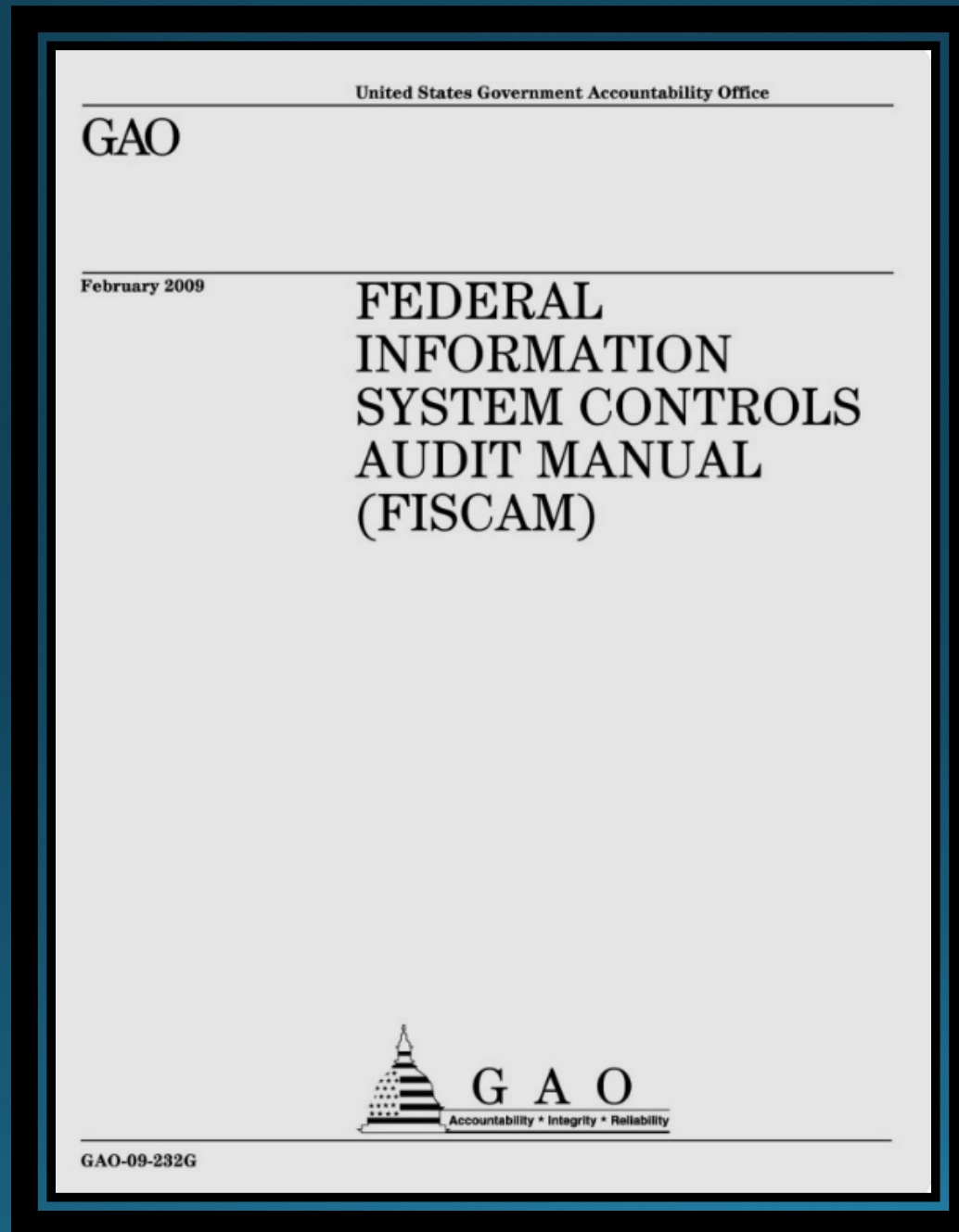


Source: insta\_photos/stock.adobe.com.

COVID-19:  
Selected Agencies Overcame  
Technology Challenges to Support  
Telework but Need to Fully Assess  
Security Controls. GAO-21-583  
Published: Sep 30, 2021.



# Why is FISCAM being updated?



# FISCAM Revision

The 2009 FISCAM content has been reorganized to

- (1) follow the planning, testing, and reporting phases of an engagement and
- (2) move the tables containing the critical elements, control activities, control techniques, and audit procedures for each general and application control category to an appendix.

This appendix has tentatively been re-branded as the FISCAM objectives-based control framework or FISCAM framework.

- Section 100 – Introduction
- Section 200 – Planning
- Section 300 – Testing
- Section 400 – Reporting
- Section 500 – Appendices

# FISCAM Time Frames

- Exposure Draft – anticipated release summer 2022
- Final Publication – TBD



# Cybersecurity Audit Methodology Manual

## Four major cybersecurity challenge areas

<p><b>Establishing a comprehensive cybersecurity strategy and performing effective oversight</b></p>	<p><b>Securing federal systems and information</b></p>	<p><b>Protecting cyber critical infrastructure</b></p>	<p><b>Protecting privacy and sensitive data</b></p>
<p>Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.</p>	<p><sup>5</sup> Improve implementation of government-wide cybersecurity initiatives.</p>	<p><sup>8</sup> Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).</p>	<p><sup>9</sup> Improve federal efforts to protect privacy and sensitive data.</p>
<p>Mitigate global supply chain risks (e.g., installation of malicious software or hardware).</p>	<p><sup>6</sup> Address weaknesses in federal agency information security programs.</p>		<p><sup>10</sup> Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.</p>
<p>Address cybersecurity workforce management challenges.</p>	<p><sup>7</sup> Enhance the federal response to cyber incidents.</p>		
<p>Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).</p>			

# Cybersecurity Audit Methodology Manual

New and experienced auditors can use the new IT cybersecurity audit methodology manual for FISMA and cybersecurity related audits.

The control activities listed in this manual are consistent with: the NIST Cybersecurity Framework (CSF), NIST 800-53 Rev. 5, other NIST publications, and Office of Management and Budget cybersecurity control-related policies and guidance, among others.

The procedures listed in the Cybersecurity Audit Methodology Manual are intended to be flexible, provide a framework and starting point to assess the enhanced security requirements, and can be tailored to the needs of the auditor.

# Features



Crosswalks to the NIST  
Cybersecurity Framework and NIST  
800-53 Rev. 5 controls

Crosswalks to GAO's Green Book  
and Yellow Book

NIST CSF-based suggested audit  
steps



# Draft Outline

- **Chapter 1.** Use and Application. Who will use this manual and what is the purpose.
- **Chapter 2.** General Planning. How to plan for the audit.
- **Chapter 3.** Audit Steps. Suggested detail audits steps for areas such as: assets and risk management; protecting systems and information; logging and monitoring; incident response; and contingency planning.
- **Appendixes**
  - NIST CSF-based suggested audit steps (Excel spreadsheet)
  - Mapping NIST CSF to Green Book (Excel spreadsheet)
  - Mapping NIST CSF to other NIST publications

# Challenges

Information Security vs. Cybersecurity

Criteria used (NIST 800-53 or NIST Cybersecurity Framework)

Detailed steps vs. high-level examples and concepts

Zero Trust Architecture

Cloud computing, FedRAMP, StateRAMP

# Cybersecurity Audit Methodology Manual Time Frames

- Draft publication – beginning of 2022
- Final Publication – summer 2022



# Differences between FISCAM and CAMM

- The *Federal Information System Controls Audit Manual (FISCAM)* revision will continue to support assessing information system controls related to financial audits, attestation engagements, and certain performance audits.
- The *Cybersecurity Audit Methodology Manual* will support both information security and cybersecurity performance audits.

# Have Feedback?

---

Team's mailbox:

[CybersecurityAuditManualUpdate@gao.gov](mailto:CybersecurityAuditManualUpdate@gao.gov)

- Jennifer R. Franks, [FranksJ@gao.gov](mailto:FranksJ@gao.gov)
- Tammi Kalugdan, [KalugdanT@gao.gov](mailto:KalugdanT@gao.gov)
- Rosanna Guerrero, [GuerreroR@gao.gov](mailto:GuerreroR@gao.gov)

# Q & A

---



# Thank you!

---

# GAO CONTACT

---

## **GAO on the Web**

Web site: <https://www.gao.gov/>

## **Congressional Relations**

Nikki Clowers, Managing Director, [clowers@gao.gov](mailto:clowers@gao.gov)  
(202) 512-4400, U.S. Government Accountability Office  
441 G Street, NW, Room 7125, Washington, DC 20548

## **Public Affairs**

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov)  
(202) 512-4800, U.S. Government Accountability Office  
441 G Street, NW, Room 7149, Washington, DC 20548

## **Copyright**

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.