Agenda

• Overview of GAO
• High Risk Report - Cybersecurity Challenges and Urgent Actions to Address Them
• GAO E-Security Lab
• Cybersecurity Audit Methodology Update
GAO’s Mission

GAO exists to support the Congress in meeting its constitutional responsibilities and to help improve the performance and ensure the accountability of the federal government for the benefit of the American people.

We provide Congress with timely information that is objective, fact-based, nonpartisan and non-ideological.
Core Values

**Accountability**
Help the Congress oversee federal programs, policies, and operations to ensure accountability to the American people.

**Integrity**
Ensure that our work is professional, objective, fact-based, nonpartisan and non-ideological.

**Reliability**
Provide high-quality, timely, accurate, useful, clear and candid information.
Evolution of Our Mission

1921: Oversee financial management processes of the Executive Branch after WWI

1970: Provide oversight of program performance & government-wide issues

2004: Expand portfolio to cover oversight, insight & foresight
The Modern GAO

- Today, performance audits, program evaluations and policy analyses account for over 90 percent of GAO’s workload
- GAO increasingly involved in a full range of oversight, insight and foresight activities
- GAO has adopted a philosophy of “leading by example” and “partnering for progress”
Three branches of U.S. Government

U.S. Constitution

EXECUTIVE
Federal Agencies

LEGISLATIVE
Congressional Research Service
Congressional Budget Office
Government Accountability Office

JUDICIAL
Comptroller General of the United States

Gene L. Dodaro

• Joint selection/appointment involving the Congress and the President
• Removed only by impeachment
• 15-year term
• Appointed on December 20, 2010
• Term will end in 2025
What did GAO accomplish in FY18?

GAO’s FY18 achievements included, among others:

- $75 billion in financial benefits
- A return of $124 for every dollar invested in GAO
- 633 reports issued containing a total of 1,650 recommendations
- 98 testimonies before 48 separate Congressional committees
GAO’s People

- GAO’s staff are civil servants; none are political appointees
- Approximately 3,000 staff
  - 70% in Washington D.C. headquarters
  - 30% in GAO’s 11 field offices
- Staff have diverse academic training
  (public policy and administration, social sciences, accounting, computer science, law, etc.)
- Certified public accountants (CPAs) conduct financial audits
# About the IT & Cybersecurity (ITC) Team

<table>
<thead>
<tr>
<th>IT Management Issues</th>
<th>Cybersecurity Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>• IT Management and Operations</td>
<td>• Cybersecurity Strategy and Oversight</td>
</tr>
<tr>
<td>• Systems Acquisition and Development</td>
<td>• Federal Cybersecurity</td>
</tr>
<tr>
<td>• IT Project Management</td>
<td>• Critical Infrastructure Cybersecurity</td>
</tr>
<tr>
<td>• Information Management</td>
<td>• Data Protection and Privacy</td>
</tr>
</tbody>
</table>
GAO’s Cybersecurity High Risk Area (introduced in 1997)

Major challenges

- Establishing a comprehensive cybersecurity strategy and performing effective oversight
- Securing federal systems and information
- Protecting critical infrastructure
- Protecting privacy and sensitive data

Critical actions needed

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

Source: GAO analysis. | GAO-18-622
Recent Report

HIGH-RISK SERIES

Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation

Page 14

Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.

Mitigate global supply chain risks (e.g., installation of malicious software or hardware).

Address cybersecurity workforce management challenges.

Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).
Challenge #1: Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight

• “[Recent] efforts provide a good foundation toward establishing a more comprehensive strategy, but more effort is needed to address all of the desirable characteristics of a national strategy.” [GAO-18-645T]

• “If global IT supply chain risks are realized, they could jeopardize the confidentiality, integrity, and availability of federal information systems.” [GAO-18-667T]

• “Agencies had not effectively conducted baseline assessments of their cybersecurity workforce or fully developed procedures for coding positions.” [GAO-18-466]

• “IoT devices that continuously collect and process information are potentially vulnerable to cyber-attacks.” [GAO-17-75]
Improve implementation of government-wide cybersecurity initiatives.

Address weaknesses in federal agency information security programs.

Enhance the federal response to cyber incidents.
Challenge #2: Securing Federal Systems and Information

• “While agencies have gotten better at preventing and detecting intrusions into their systems, they are still vulnerable to attacks such as "phishing"—emails designed to trick staff into clicking malicious links. Moreover, many agencies have not yet fully implemented effective security programs or practices, leaving them vulnerable to future attacks.” GAO-19-105

• “We reported numerous deficiencies in CDC's information security program and controls that CDC used to identify risk, protect systems, detect and respond to cybersecurity events, and recover operations after such events.” GAO-19-70
Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).
Challenge #3: Protecting Cyber Critical Infrastructure

• “The nation depends on the interstate pipeline system to deliver oil, natural gas, and more. This increasingly computerized system is an attractive target for hackers and terrorists.” GAO-19-48

• “The Department of Homeland Security (DHS) had not measured the impact of its efforts to support cyber risk reduction for high-risk chemical sector entities.” GAO-18-211

• “The federal government had identified major challenges to the adoption of the cybersecurity framework.” GAO-18-211

• “Major challenges existed to securing the electricity grid against cyber threats.” GAO-16-174
Improve federal efforts to protect privacy and sensitive data.

Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.
Challenge #4: Protecting Privacy and Sensitive Data

- “CMS and external entities were at risk of compromising Medicare Beneficiary Data due to a lack of guidance and proper oversight.” GAO-18-210
- “The Equifax breach resulted in the attackers accessing personal information of at least 145.5 million individuals.” GAO-18-559
- “The emergence of IoT devices can facilitate the collection of information about individuals without their knowledge or consent” GAO-17-75
- “Smartphone tracking apps can present serious safety and privacy risks.” - GAO-16-317
Established to meet the needs for cybersecurity assessments to support financial audits starting in 1997

Developed over 20 years to build up the current, in-house technical audit capability (rather than contract out; lower cost, greater expertise)

Conducted technical security reviews in support of numerous GAO and legislative branch efforts

Produces about 20% of GAO’s annual audit accomplishments with only 15 staff

Has evolved considerably over time to meet other agency needs (e.g., multiple sandboxes, secure data transfer, advanced analytics capability)
ARM E-Security Lab: Enhancing GAO’s Cybersecurity Audit Function: Synergy

ARM Data Facility

ARM Test Network

Maintain, upgrade, administer and support user community of ADF systems

Technical Skill Set Increases

Test audit tools & techniques, develop & test scripts, and conduct proof of concept testing

Cybersecurity Assurance

 Organizations of Audit Interest

GAO’s credibility enhanced to conduct reviews of highly complex, technical, interconnected computing environments
INFORMATION SECURITY

Significant Progress Made, but CDC Needs to Take Further Action to Resolve Control Deficiencies and Improve Its Program
Graph showing the number of open recommendations over time, from March 2018 to September 2020. The graph indicates a significant reduction in open recommendations over the period, with specific numbers at various points, such as 184 open as of the release of the LOUO report on June 20, 2018, and 2 open as of September 2020.

Source: GAO analysis of Centers for Disease Control and Prevention data. | GAO-19-70
GAO’s FISCAM

• Federal Information Systems Controls Audit Manual
• Methodology to support financial and performance audits in accordance with GAGAS
• Last issued 2009
• In process of revision to align with current NIST guidance
• Will be seeking input from numerous stakeholders (including NIST)