GAO Update: Cybersecurity

Vijay D'Souza
Director

Nick Marinos
Director

Information Technology & Cybersecurity
U.S. Government Accountability Office

May 2019

Agenda

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

Overview – U.S. GAO

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

General Accounting Office established

Legal name becomes Government Accountability Office

1921 — 1970 — 2004

Oversee financial management processes of the Executive Branch after WWI

+

Provide oversight of program performance & government-wide issues

+

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

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

GAO

About the IT & Cybersecurity (ITC) Team

IT Management Issues

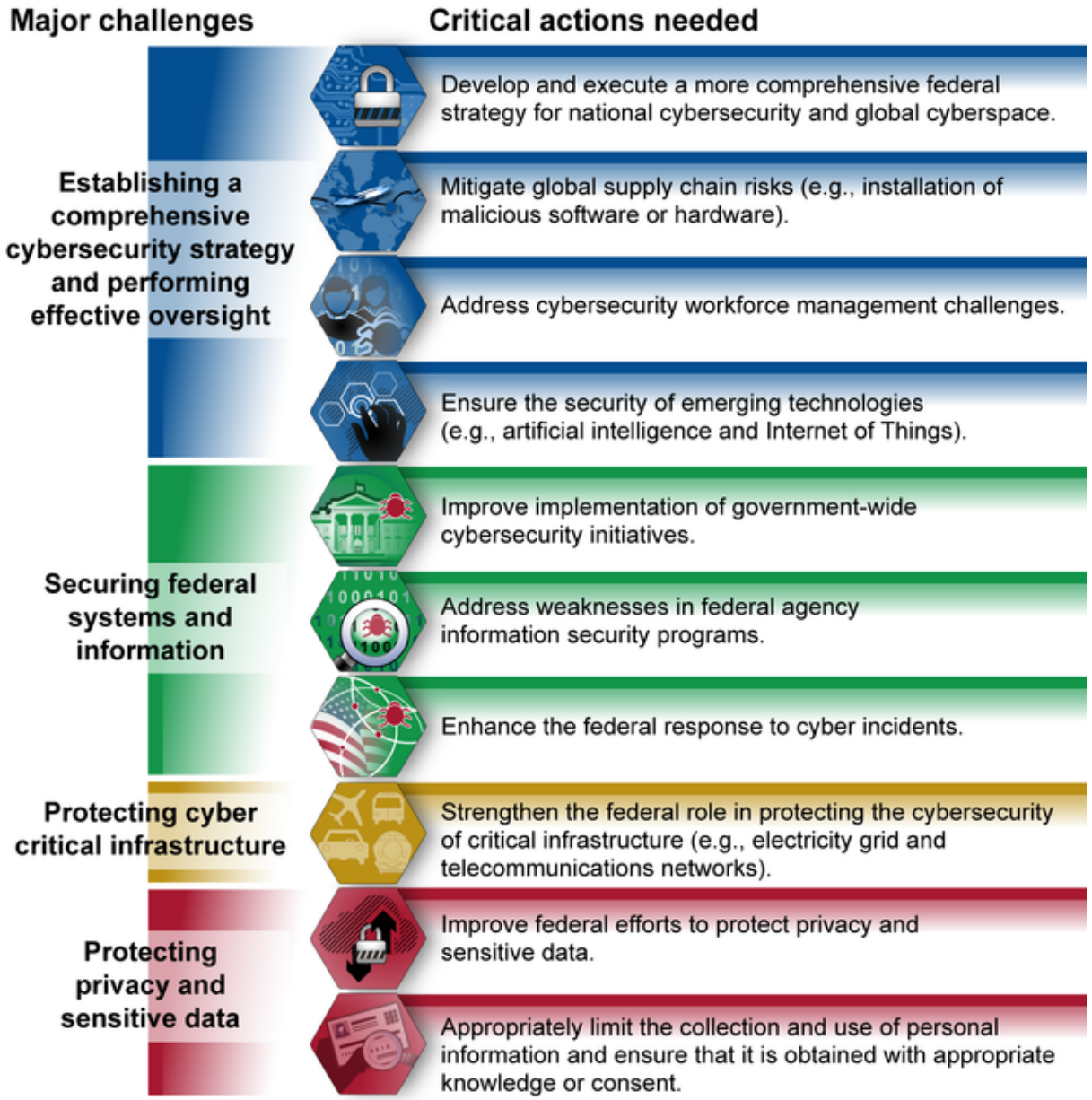
- IT Management and Operations
- Systems Acquisition and Development
- IT Project Management
- Information Management

Cybersecurity Issues

- Cybersecurity Strategy and Oversight
- Federal Cybersecurity
- Critical Infrastructure Cybersecurity
- Data Protection and Privacy

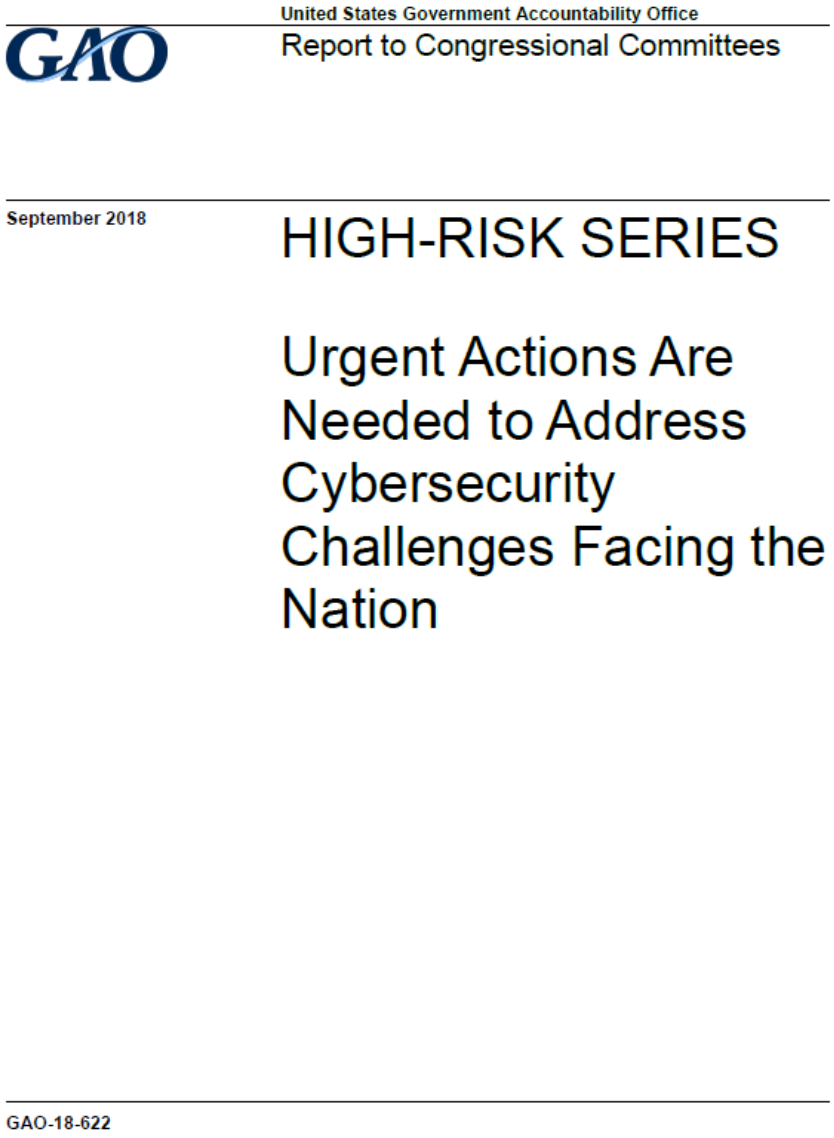
ITC INFORMATION TECHNOLOGY & CYBERSECURITY TEAM

GAO's Cybersecurity High Risk Area *(introduced in 1997)*



Source: GAO analysis. | GAO-18-622

Recent Report


United States Government Accountability Office

Report to Congressional Committees

September 2018

HIGH-RISK SERIES

Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation

GAO-18-622

http://www.gao.gov/products/GAO-18-622

GAO

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).

GAO

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

GAO

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).

GAO

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.

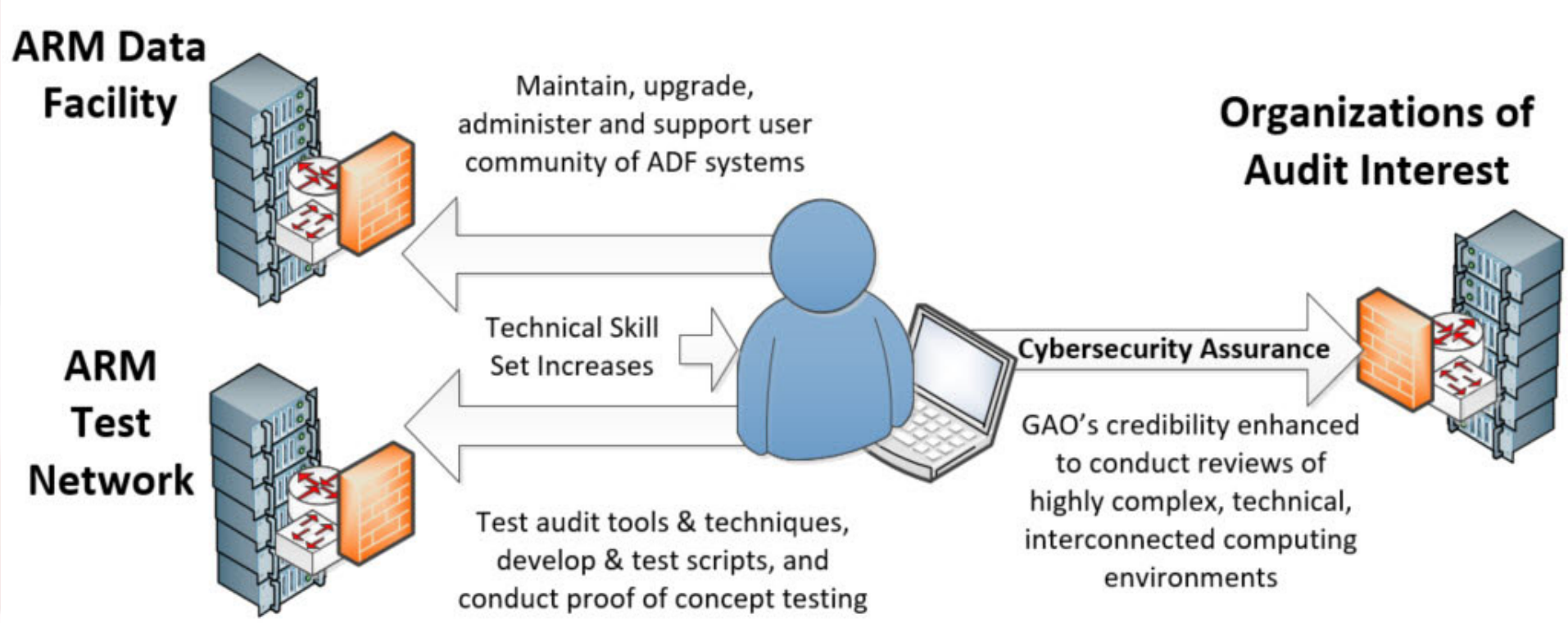
Challenge #4: Protecting Privacy and Sensitive Data

- "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

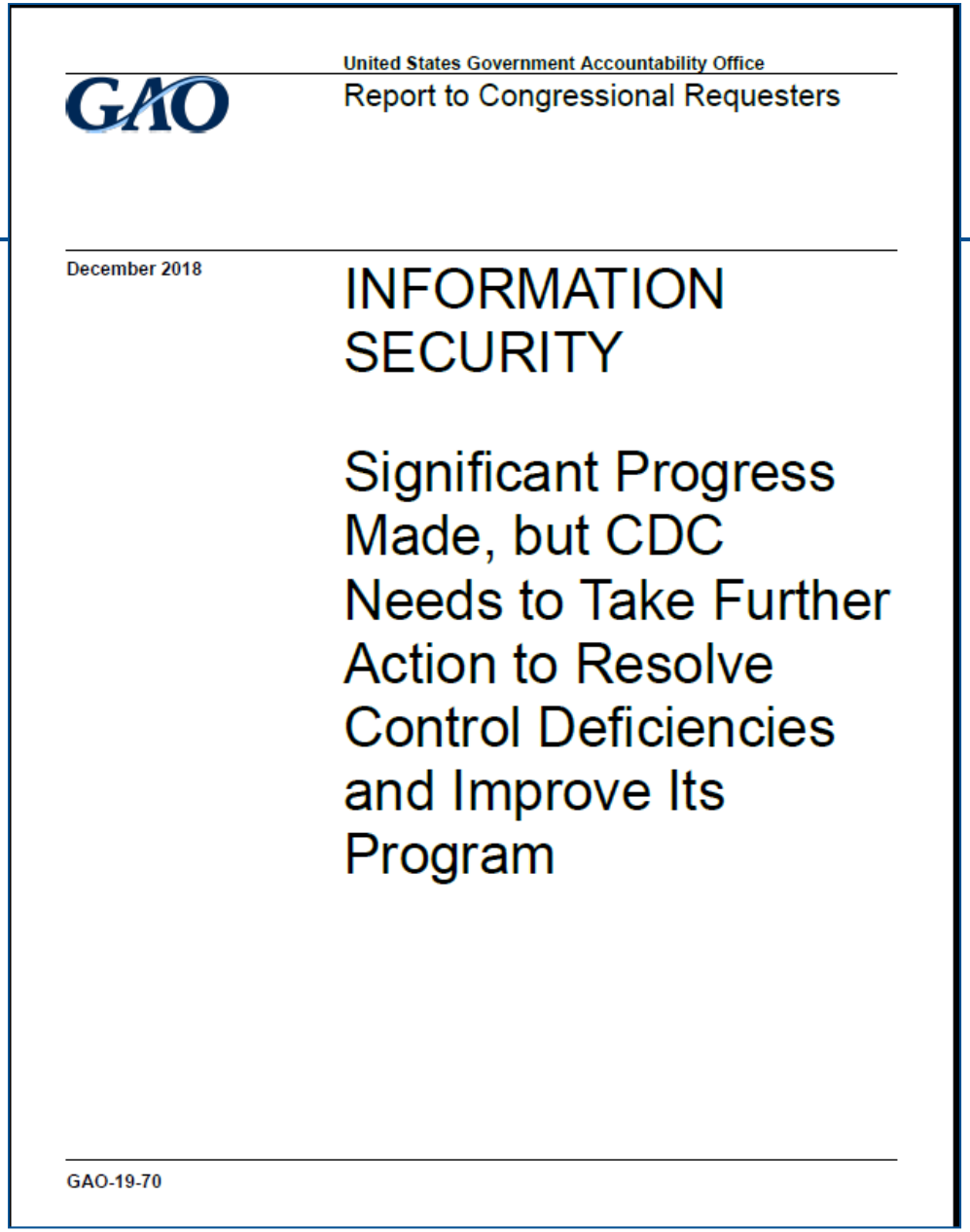
GAO E-Security Lab: Enhancing GAO's Cybersecurity Audit Function

- 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



Recent Reports



United States Government Accountability Office

Report to Congressional Requesters

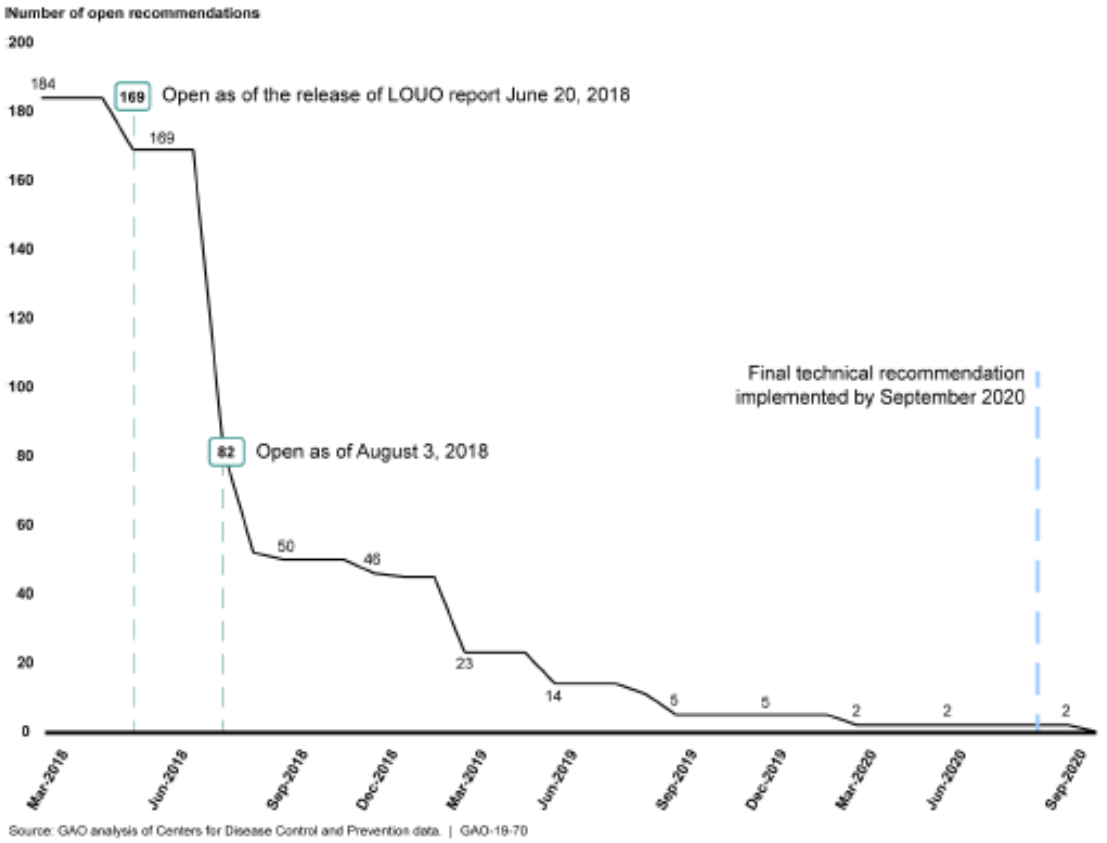
December 2018

INFORMATION SECURITY

Significant Progress Made, but CDC Needs to Take Further Action to Resolve Control Deficiencies and Improve Its Program

GAO-19-70

https://www.gao.gov/products/GAO-19-70



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)

GAO on the Web

Web site: http://www.gao.gov/

Congressional Relations

Orice Williams Brown, Managing Director, williamso@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
(202) 512-4800, U.S. Government Accountability Office
441 G Street, NW, Room 7149, Washington, DC 20548

Copyright

GAO on the Web

Web site: http://www.gao.gov/

Congressional Relations

Orice Williams Brown, Managing Director, williamso@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
(202) 512-4800, U.S. Government Accountability Office
441 G Street, NW, Room 7149, Washington, DC 20548

Copyright