GAO

Shaping the Future of
Government Auditing Joint Meeting

# Cybersecurity Challenges Facing the Nation and How Auditors Can Help

*August 13, 2019*

# Agenda

- GAO, ITC and IT Auditing
- Challenges Facing the Nation
- How Auditors Can Help
- Questions and Answers

# Professional Me

## Vijay D’Souza

Director, Information Technology and Cybersecurity Team

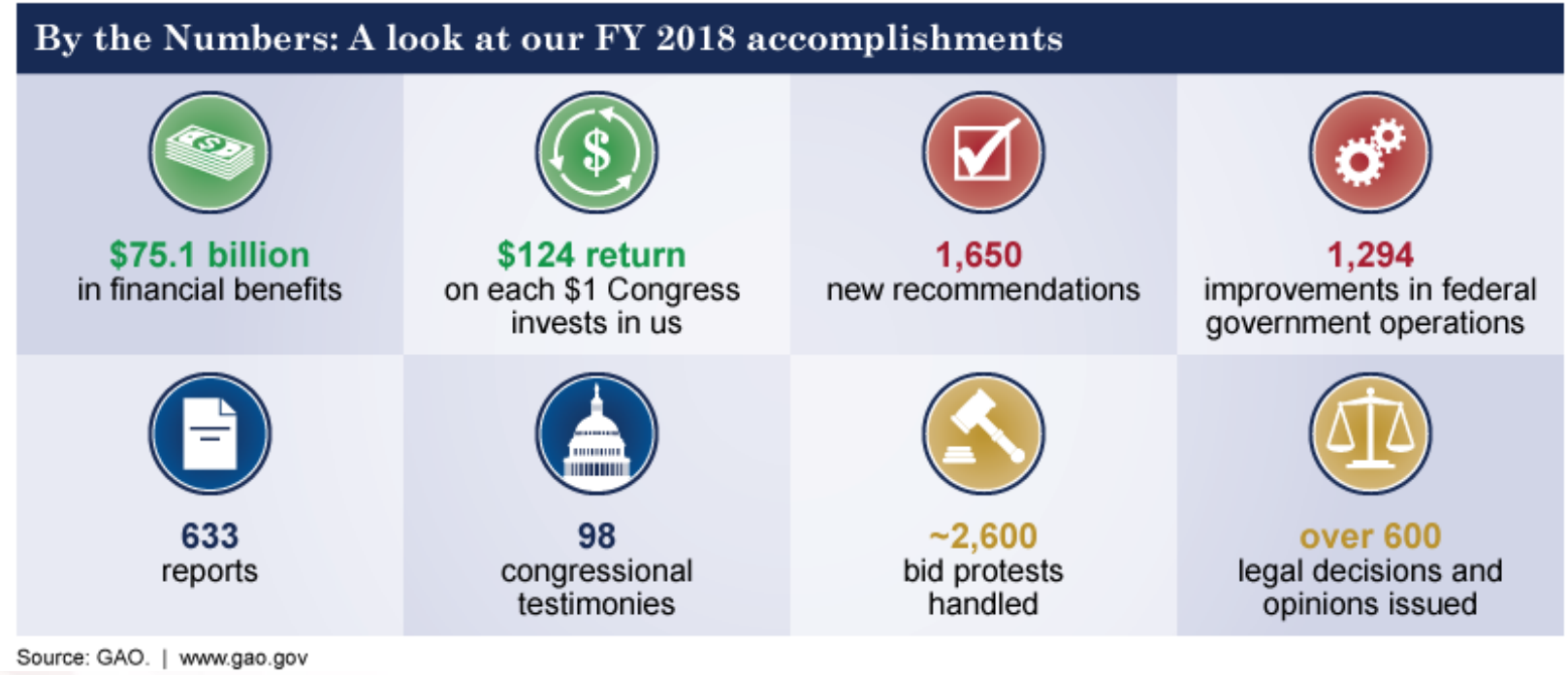
Prior experience

- Data analytics
- Health Care auditing
- Technical writing

# Who Is GAO

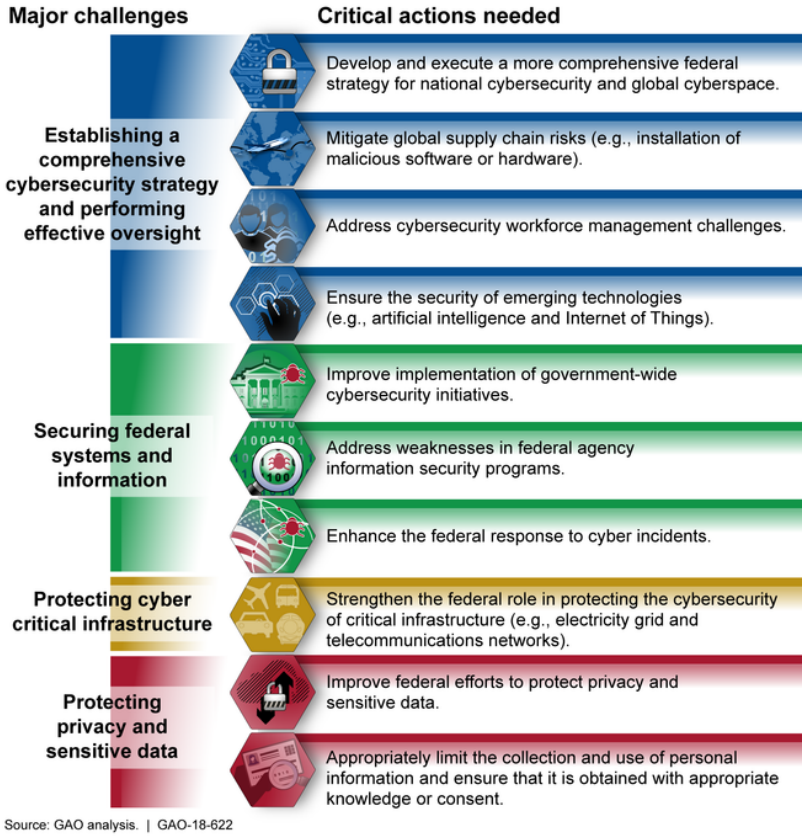
- Serve Congress
- Oversight Mission
- Nonpartisan Source of Objective Information

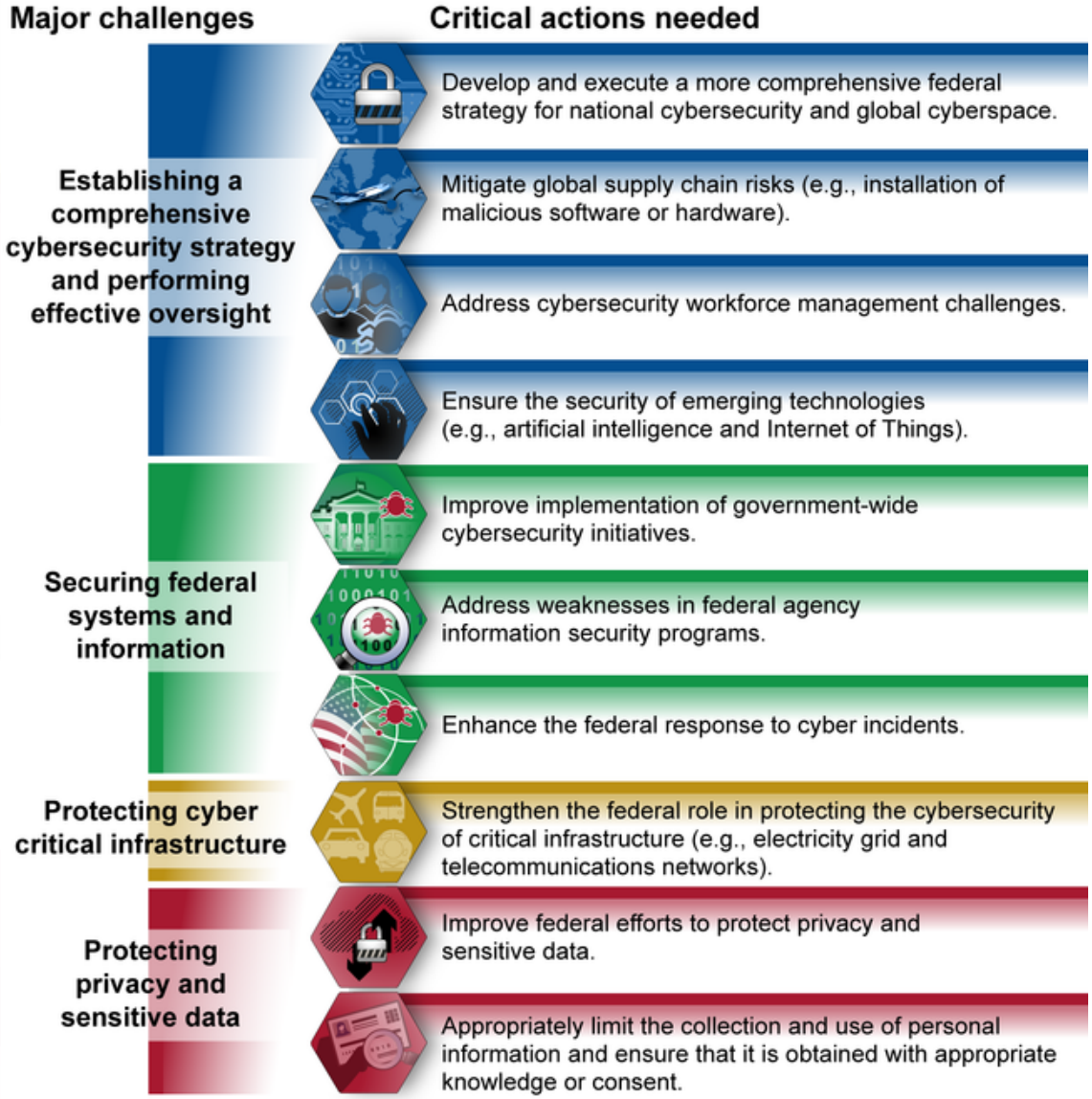
# Key Stats


By the Numbers: A look at our FY 2018 accomplishments
$75.1 billion
in financial benefits
$124 return
on each $1 Congress
invests in us
1,650
new recommendations
1,294
improvements in federal
government operations
633
reports
98
congressional
testimonies
~2,600
bid protests
handled
over 600
legal decisions and
opinions issued
Source: GAO. | www.gao.gov

# GAO's Cybersecurity High Risk Area


Introduced in 1997



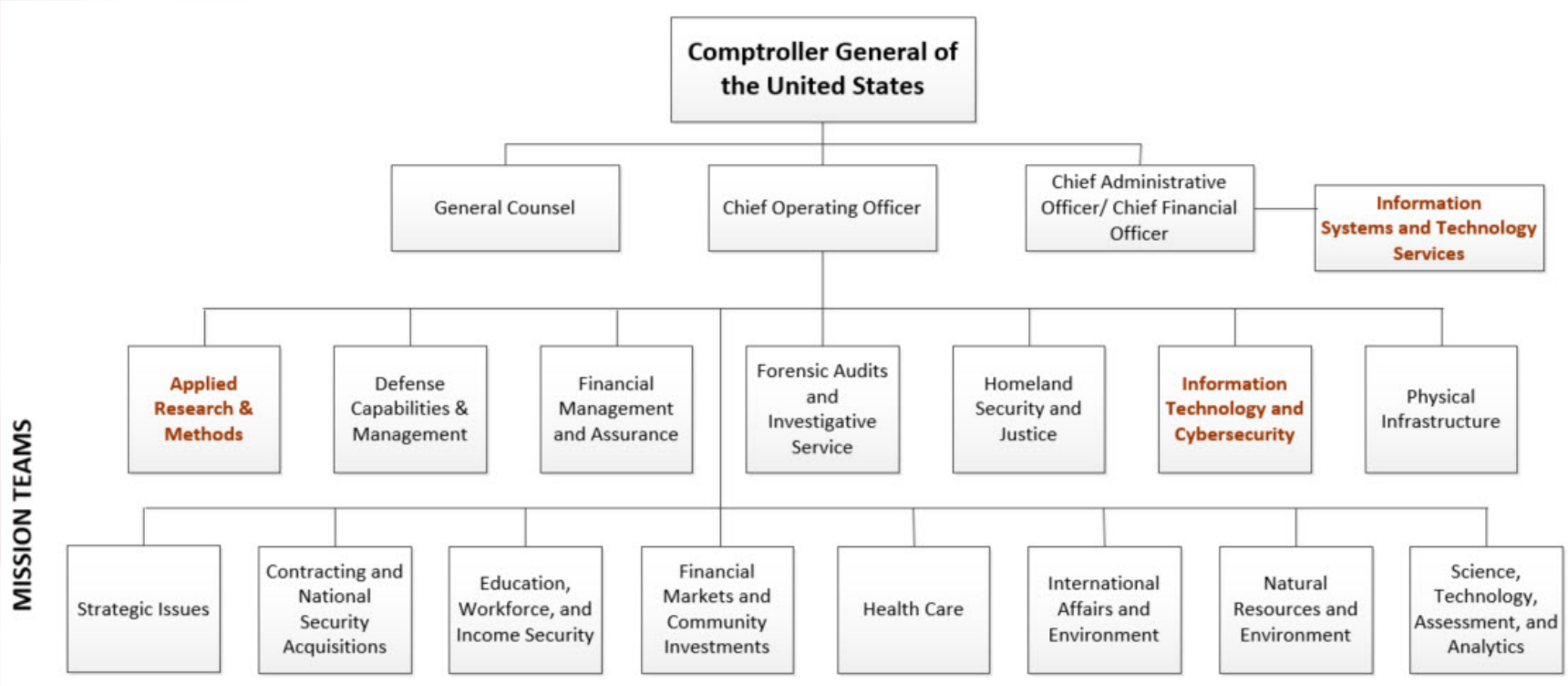



Source: GAO analysis. | GAO-18-622

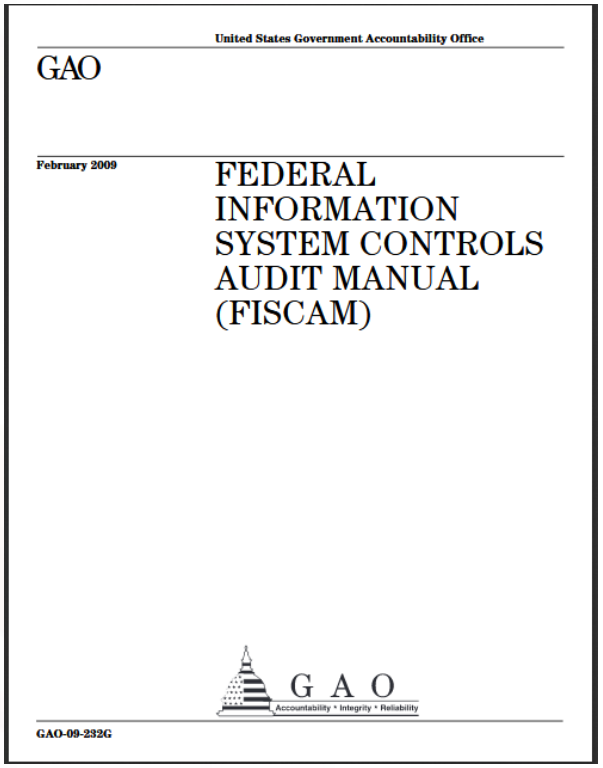
# Recent Changes

- Recent reorganization to emphasize science and technology
- Emphasis on cybersecurity
- Increased matrixing because of interconnected nature of cyber issues

# Organization



# Federal Information System Controls Audit Manual


United States Government Accountability Office

GAO

February 2009

FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL (FISCAM)

GAO

Accountability * Integrity * Reliability

GAO-09-232G

GAO's methodology for auditing information system controls in federal and other government entities.

# Recent and Ongoing Work

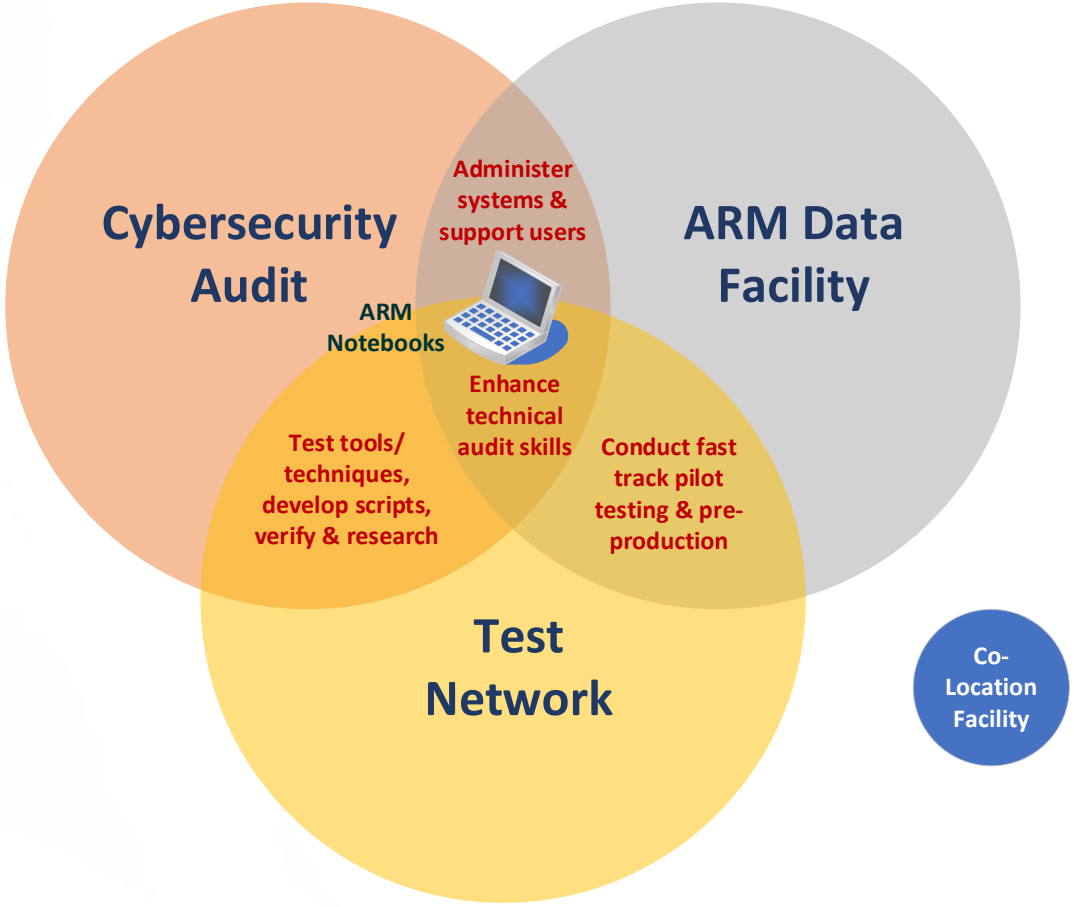
- Train Control
- Cybersecurity Risk Management
- VA Electronic Health Records
- 2020 Census
- IRS Financial Systems
- Legacy System Costs
- Election Security
- IPv4 to IPv6 transition
- Medicaid IT System Spending

# Information Technology & Cybersecurity (ITC)

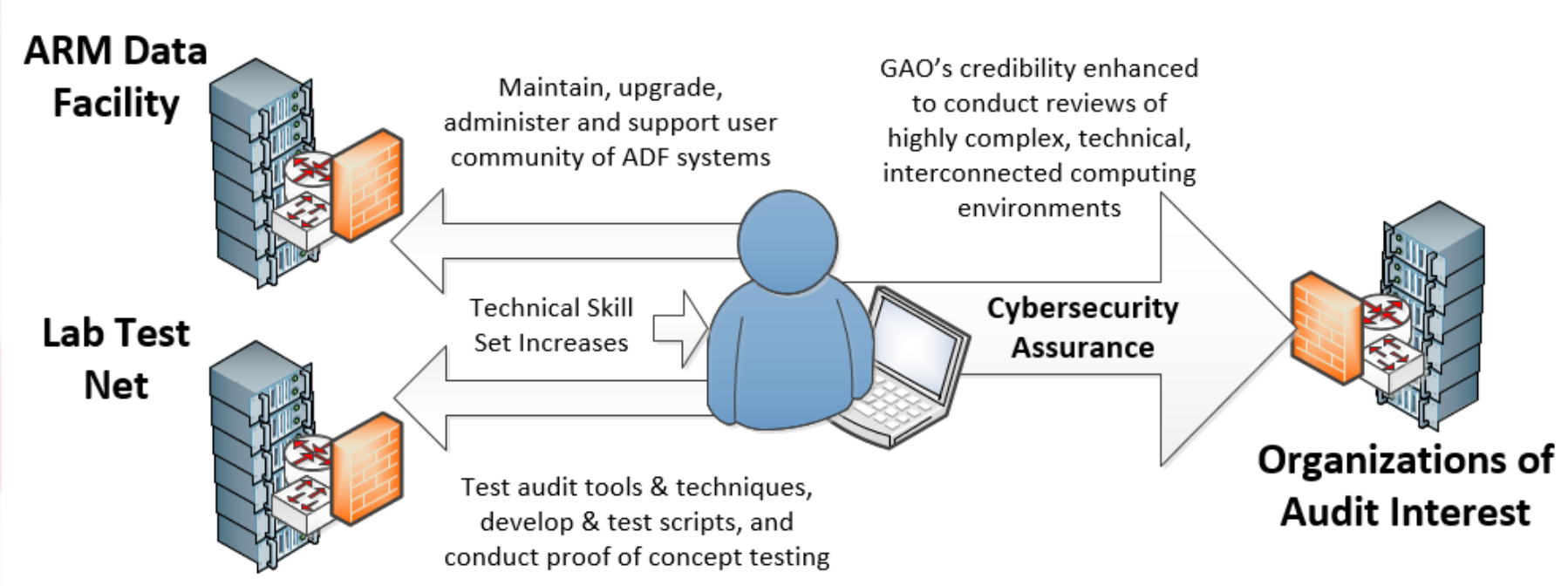
- GAO created the e-Security Lab in 1997 to provide a responsive in-house technical capability to conduct cybersecurity assurance audits
- Beginning in FY2020, the Lab will become part of the ITC team and be known as the Center for Enhanced Security and Computing (CESC)

## Introduction and Background

# CESC (formerly known as the e-Security Lab)



# Creating Mission Synergy



# Challenges Facing the Nation

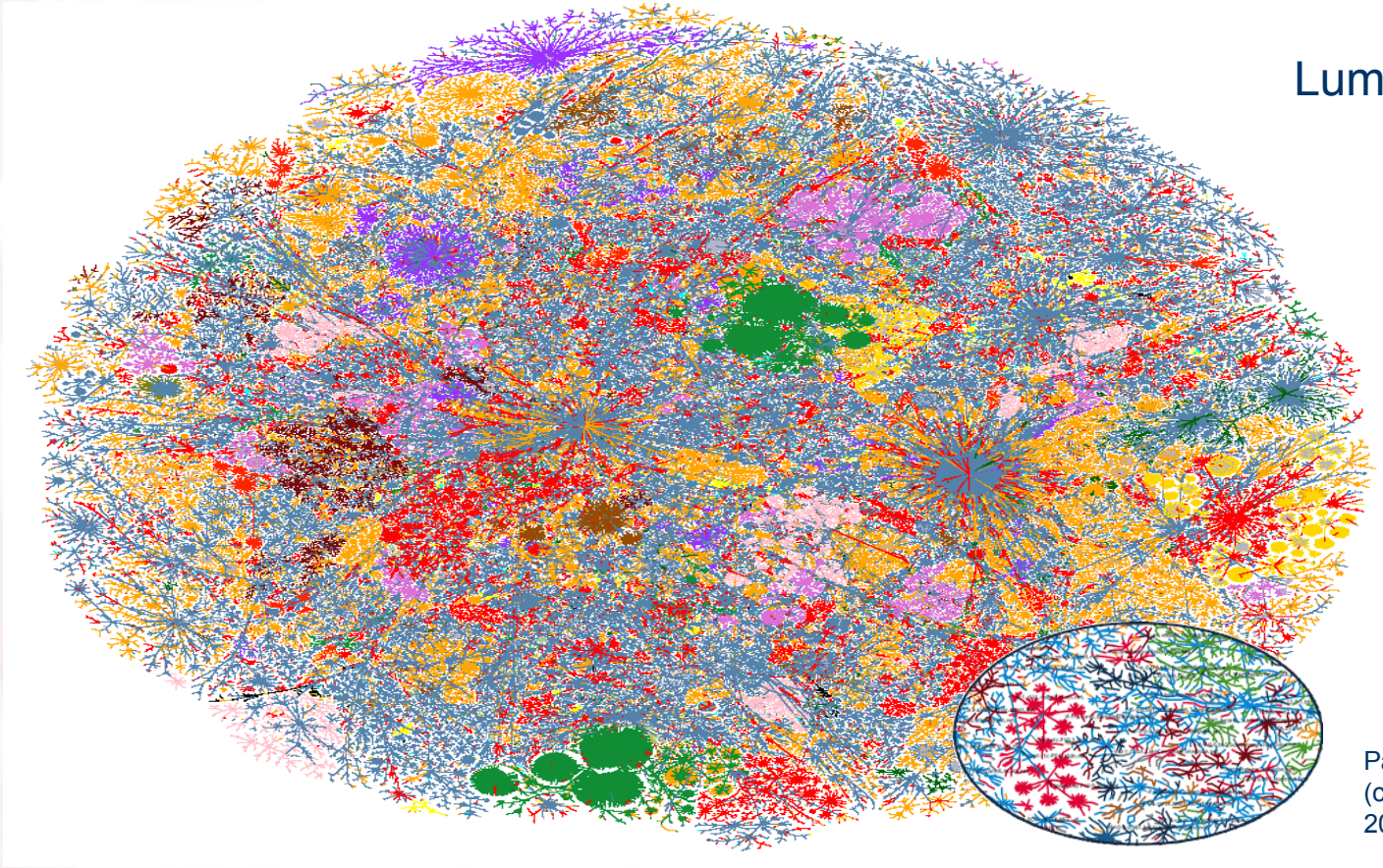
# Challenges Facing the Nation

**Problem Statement:**

How do we secure everything, from everyone, all the time, whereas … an adversary only has to get it right once.

(paraphrasing Tony Sager, formerly of NSA)

# Internet Map



Lumeta Corporation's Internet Map

# IT Audit – Skills Gap

- Understanding networks and information systems that are becoming more complex, diverse & interconnected
- Staying current with evolving technologies

# IT Audit – Skills Gap

- Internet of Things
- Cloud Computing
- Blockchain Technology
- Supply Chain
- Artificial Intelligence
- Etc …

# IT Audit - Methodology

Traditional types of IT audits not as effective in new computing environments, i.e., limited scope reviews, use of compliance checklists, vulnerability scanning, and penetration testing.

# IT Audit - Resources

- Test networks, commercial tools and specialized training can be costly
- Recruiting, maintaining and retaining an effective IT audit work force

# Building & Retaining Skilled Staff

# How Auditors Can Help

# Understanding Risks

What are we securing

… from whom
…. for how long
…, and at what cost

(paraphrasing Keith Rhodes, formerly of GAO)

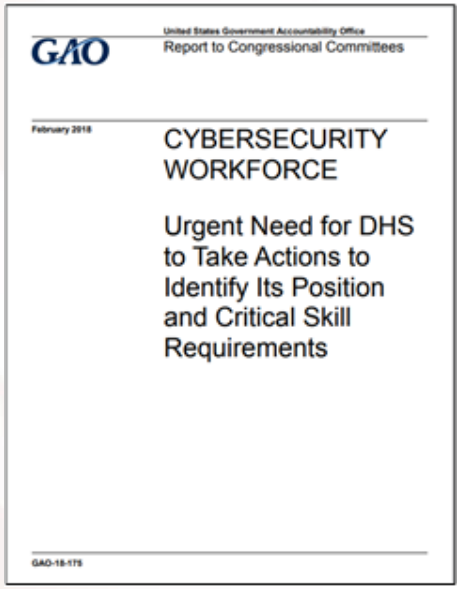
# Matrix Management (examples)






- GAO performs or oversees annual financial audits for several financially oriented federal agencies
- Combination of financial auditors, IT auditors, and issue area experts

# Matrix Management (examples)


United States Government Accountability Office
Report to Congressional Committees

February 2018

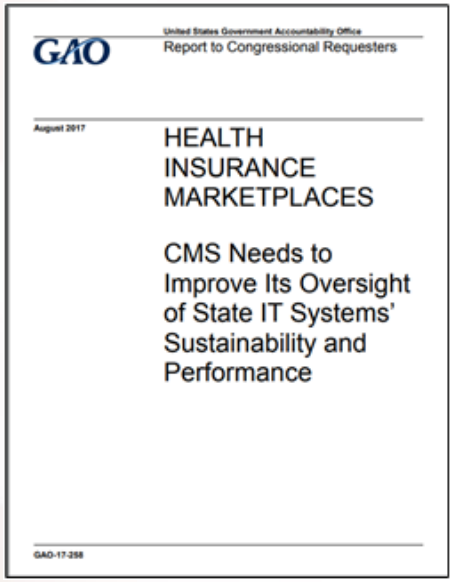
CYBERSECURITY WORKFORCE

Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements

GAO-18-175

- Tracking and categorization of cybersecurity roles in federal govt
- IT specialists brought cybersecurity knowledge
- Non-IT specialists brought knowledge of surveys, personnel rules and data, and human capital issues

# Matrix Management (examples)


United States Government Accountability Office

Report to Congressional Requesters

August 2017

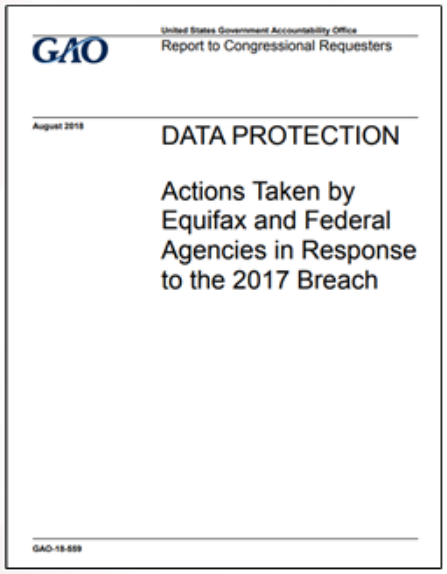
HEALTH INSURANCE MARKETPLACES

CMS Needs to Improve Its Oversight of State IT Systems' Sustainability and Performance

GAO-17-358

- How were funds being overseen to develop health insurance marketplaces?
- IT knowledge of system development and management processes
- Health care knowledge of insurance rules/regs
- State auditor knowledge of state-specific issues

# Matrix Management (examples)


United States Government Accountability Office
Report to Congressional Requesters

August 2018

DATA PROTECTION

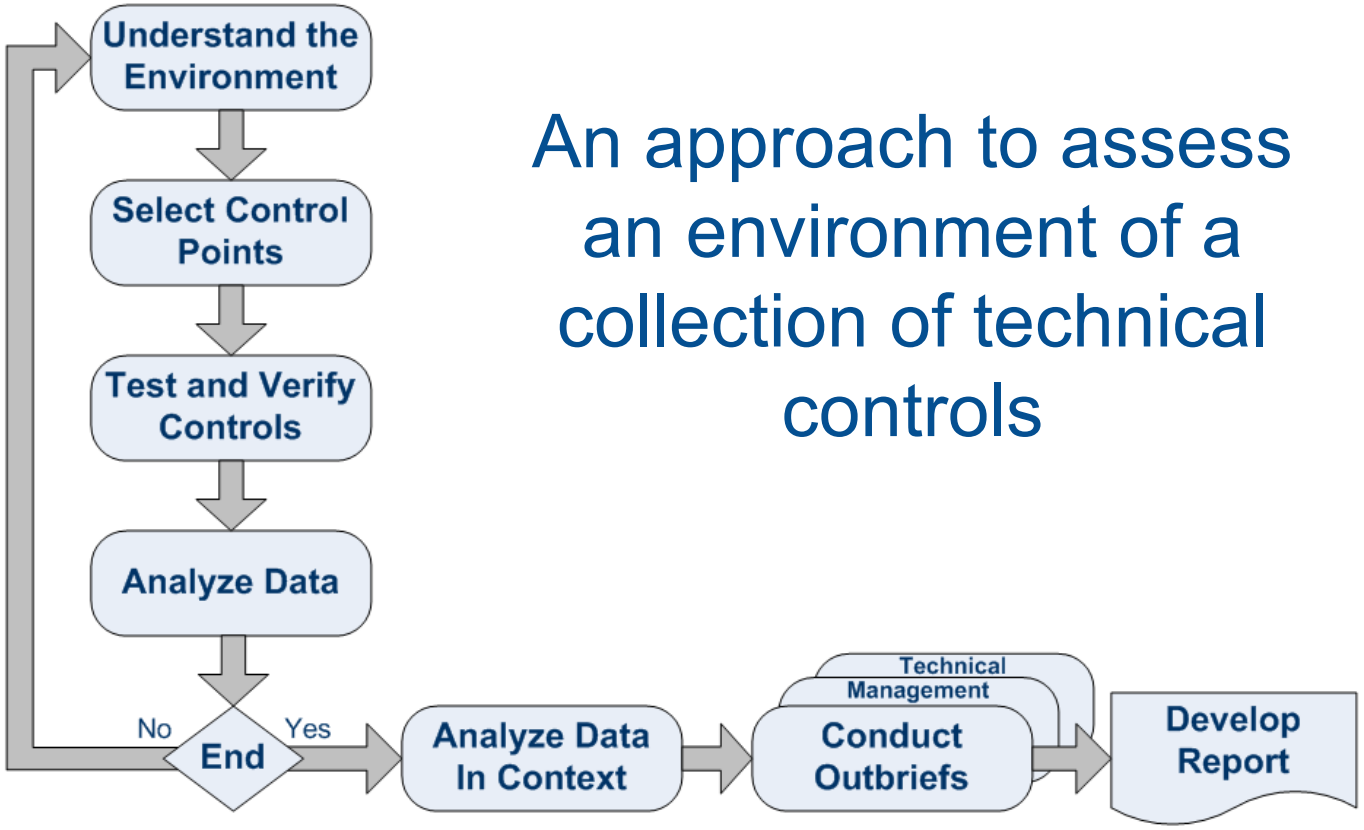
Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach

GAO-18-559

- Causes of data breach
- Impact on consumers and federal agencies
- IT specialists provided knowledge of cybersecurity issues related to data breach
- Non-IT specialists provided knowledge of federal agencies, consumer protection laws and financial markets

# Thinking about IT Auditing

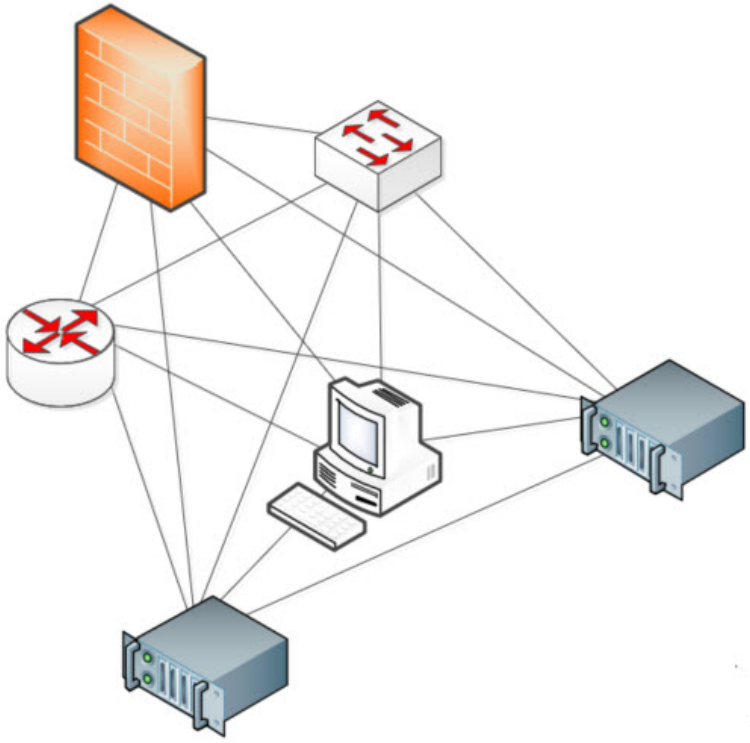
# A Holistic Iterative Approach




An approach to assess an environment of a collection of technical controls

# Understanding Trust and Dependencies

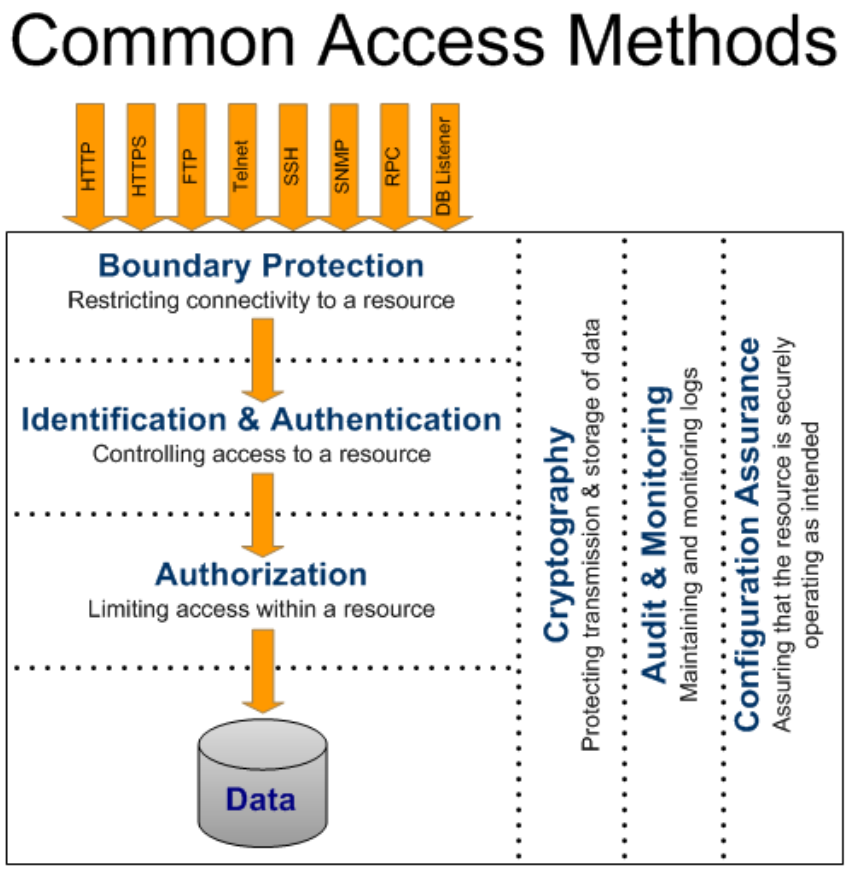
## Interconnectivity – Internal & External



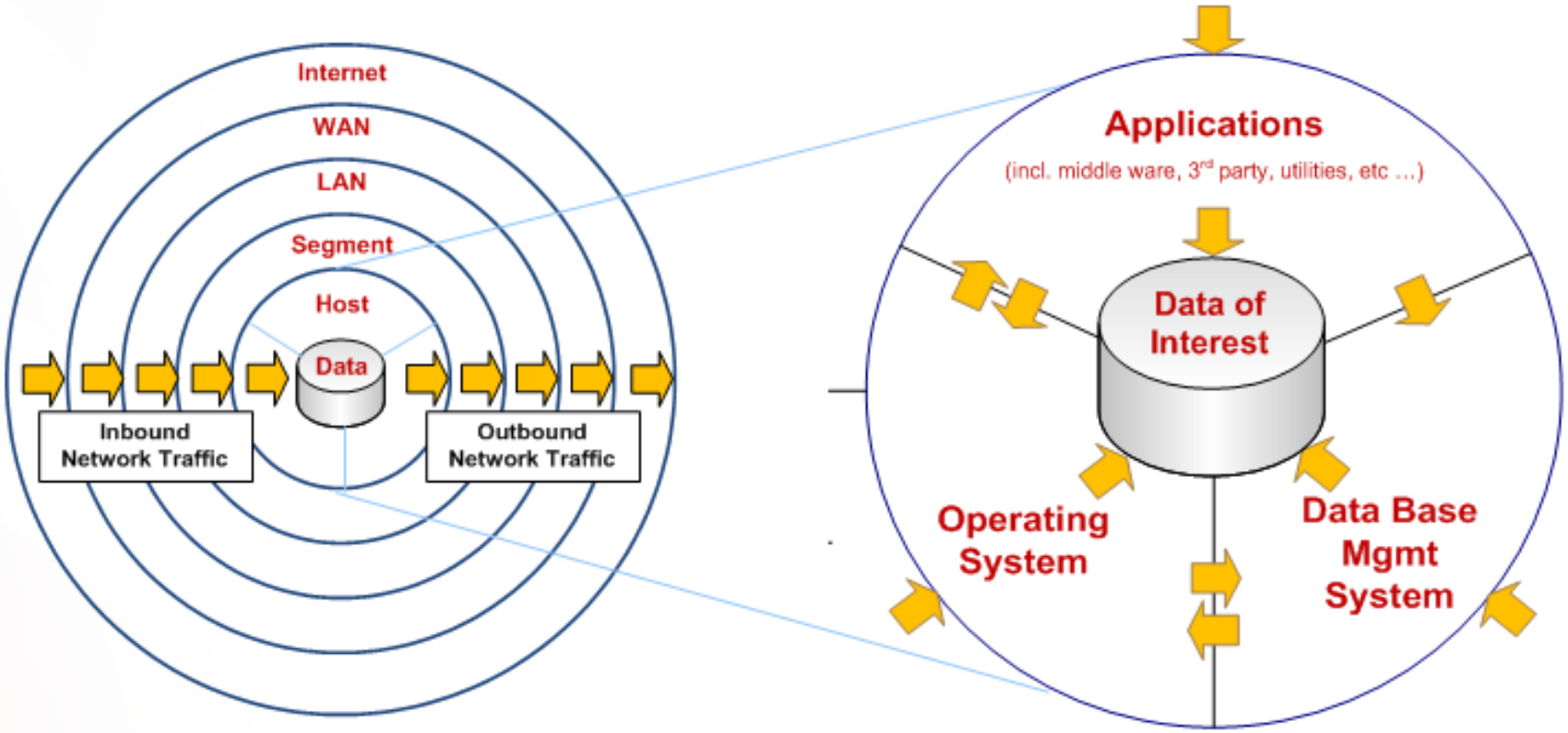
## Privilege Accounts

Operating System
Active Directory
Firewall / Network
Domain Name Server
Web Server
Host Firewall
Anti-Virus / Malware
eMail
Database
Applications
Local
Etc …

# Follow the Wire (things to consider)



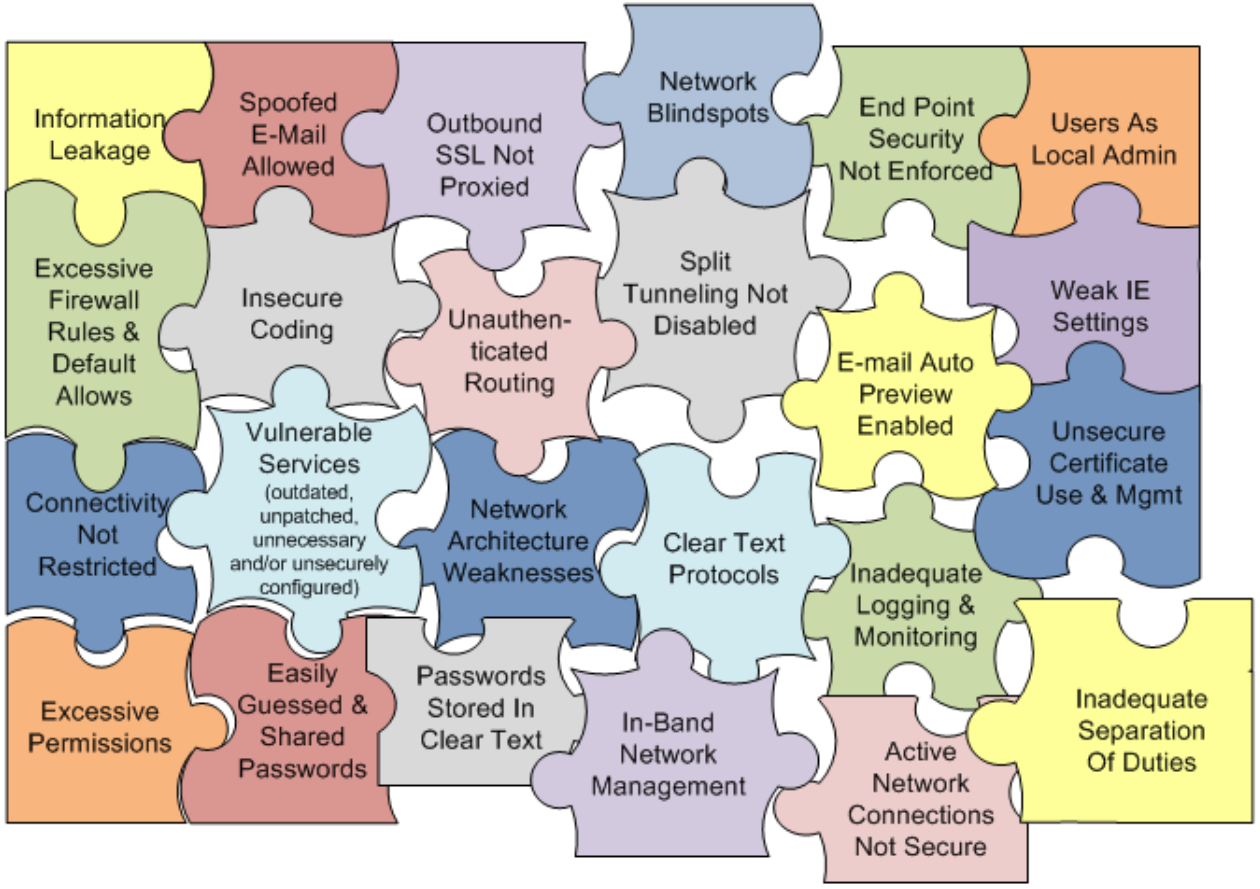
# Controlling Access



GAO

How Can IT Auditors Help

# Analyze Results in Context



GAO

# In Closing

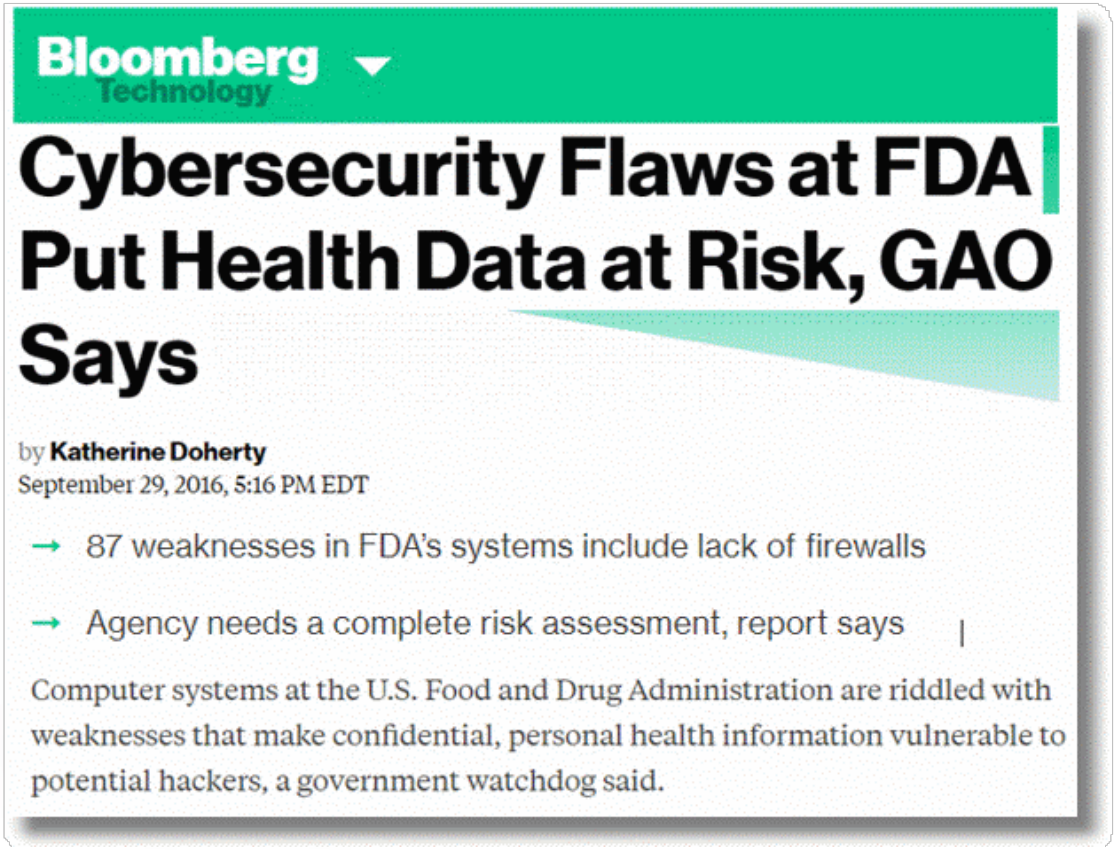
When auditing an environment of physical and virtual, diverse and interconnected controls, the answer is not always binary or easy. Consider:

- It depends
- So what
- Not all bad passwords equal in terms of effect
- It's all about context, context, context
- Adding value

# Questions and Answers

**Director, ITC**
Vijay D'Souza, DsouzaV@gao.gov

# Results in the News



Bloomberg Technology

## Cybersecurity Flaws at FDA Put Health Data at Risk, GAO Says

by **Katherine Doherty**
September 29, 2016, 5:16 PM EDT

- 87 weaknesses in FDA's systems include lack of firewalls
- Agency needs a complete risk assessment, report says

Computer systems at the U.S. Food and Drug Administration are riddled with weaknesses that make confidential, personal health information vulnerable to potential hackers, a government watchdog said.