Cybersecurity Challenges Facing the Nation and How Auditors Can Help

Nick Marinos
Director, Cybersecurity & Data Protection Issues

Information Technology Team
U.S. Government Accountability Office

November 1, 2018

Agenda

- Introduction to GAO's IT Team & Cybersecurity Audit Strategy
- The High-Risk List & Cybersecurity
- Cybersecurity Challenges and Urgent Actions to Address Them
- How GAO Scopes Cybersecurity and Privacy Audits
- Ongoing & Upcoming Work
- Challenges in Evaluating Cybersecurity
- Questions that Keep Coming up on the Audit Trail
- Emerging Issues

GAO 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.

GAO's 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.

About the IT Team: Audit Areas

- Investment Management/Governance
- IT Human Capital
- Systems Acquisition & Development
- Enterprise Architecture
- Cost & Schedule Estimation
- Telecommunications
- Emerging Technologies
- Federal Cybersecurity
- Information Management
- Privacy & Data Protection
- Cyber Critical Infrastructure Protection
- Financial Systems Security

GAO's Cybersecurity Audit Strategy

Establishing a national cybersecurity strategy and effective government-wide action and oversight

- Evaluate efforts to develop and implement a national cybersecurity strategy
- Assess federal efforts to address global cyber challenges, including cyber defense and response efforts
- Examine the implementation of government-wide cybersecurity initiatives

Ensuring the effectiveness of agency programs for the protection of federal information and systems

- Report to Congress on the effectiveness of federal agency cybersecurity
- Assess the effectiveness of security programs, policies, practices, and controls
- Evaluate the cybersecurity of major systems development and acquisition
- Assess agency preparedness for, an response to, breaches of sensitive government information

Strengthening the federal role in the public-private partnership for the protection of critical infrastructure and sensitive data

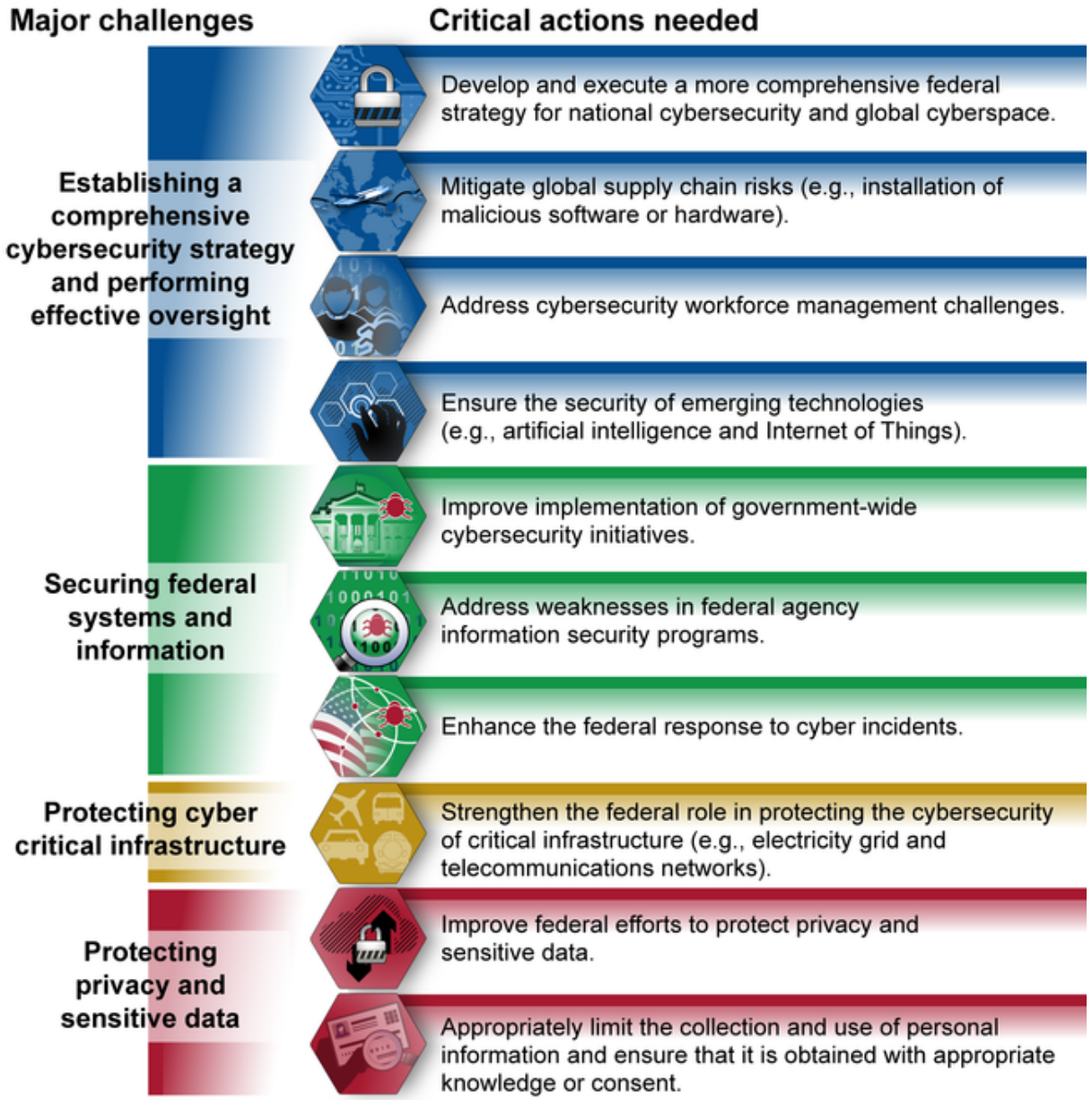
- Study cybersecurity implication of emergency technologies (IoT, Artificial Intelligence)
- Evaluate federal oversight of programs supporting the nation's critical infrastructure
- Examine federal efforts to oversee safeguarding of personal and other sensitive data shared with private-sector and other non-federal entities
- Examine federal response to security incidents with national ramifications, such as cyberattacks and data breaches at critical infrastructure components

GAO's High Risk List

- Every 2 years at the start of a new Congress, GAO calls attention to agencies and program areas that are high risk due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or are most in need of transformation.

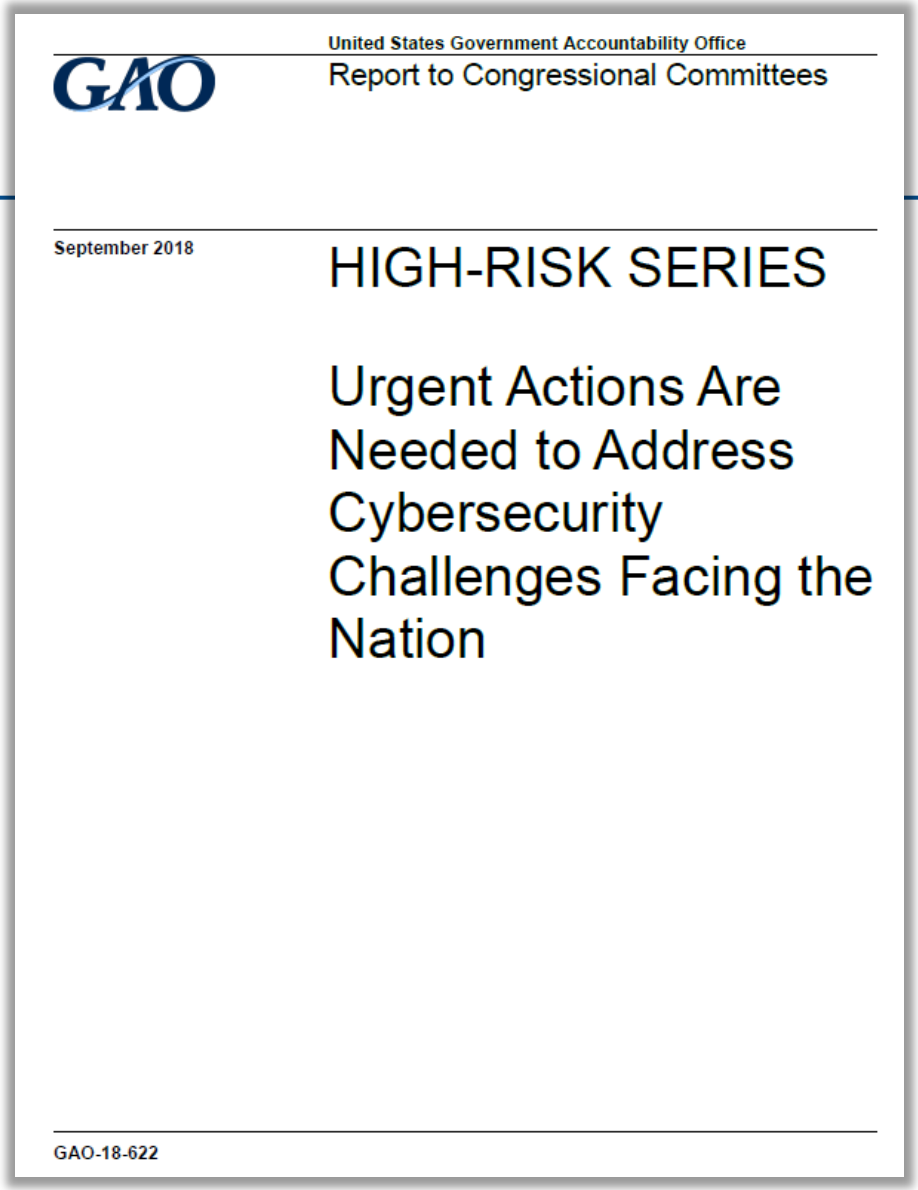
GAO

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

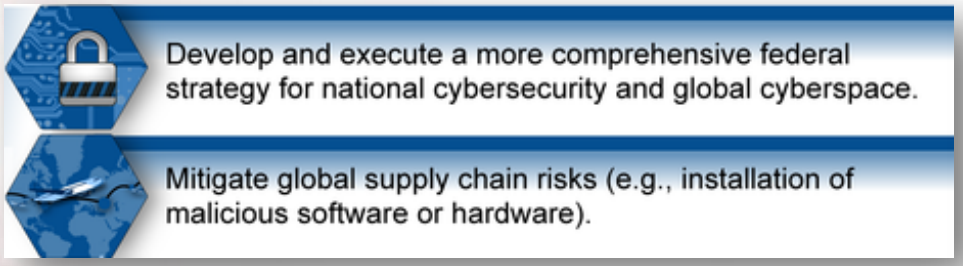
http://www.gao.gov/products/GAO-18-622

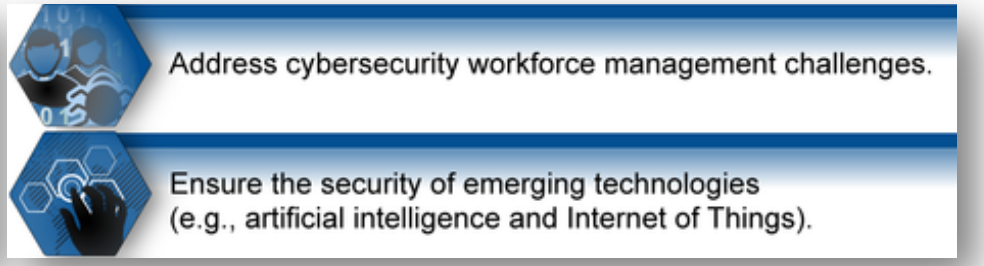
Challenge #1: Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight

- The federal government and the nation's critical infrastructure are dependent on IT systems and electronic data, which make them highly vulnerable to a wide and evolving array of cyber-based threats.
- Securing these systems and data is vital to the nation's security, prosperity, and well-being.
- The federal government has been challenged in establishing a comprehensive strategy to provide a framework for how the United States will engage both domestically and internationally on cybersecurity related matters.
- We have also reported on challenges in performing oversight, including monitoring the global supply chain, ensuring a highly skilled cyber workforce, and addressing risks associated with emerging technologies.

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."** - *Recent Testimony by the Comptroller General,* GAO-18-645T
- **"If global IT supply chain risks are realized, they could jeopardize the confidentiality, integrity, and availability of federal information systems."** *–Information Security: Supply Chain Risks Affecting Federal Agencies,* GAO-18-667T
- **"Agencies had not effectively conducted baseline assessments of their cybersecurity workforce or fully developed procedures for coding positions."** - *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions*, GAO-18-466
- **"IoT devices that continuously collect and process information are potentially vulnerable to cyber-attacks."** - *Technology Assessment: Internet of Things: Status and implications of an increasingly connected world.* GAO-17-75



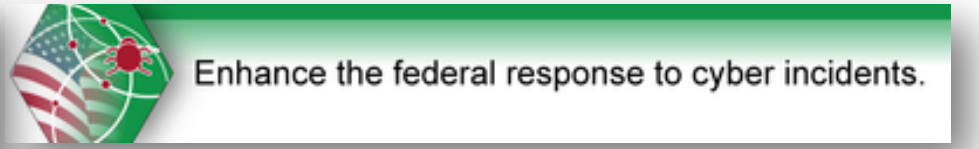


Challenge #2: Securing Federal Systems and Information

- GAO has reported that federal agencies have experienced challenges in implementing large cybersecurity initiatives, addressing weaknesses in systems and responding to cyber incidents.
- Emergence of increasingly sophisticated threats and continuous reporting of cyber incidents underscores the continuing and urgent need for effective information security.
- Federal agencies need to take appropriate steps to better ensure they have effectively implemented programs to protect their information and systems.

Challenge #2: Securing Federal Systems and Information

- **"DHS had been challenged in measuring how the NCCIC was performing its functions in accordance with mandated implementing principles."** - *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely,* GAO-17-163
- **"Federal agencies continued to experience weaknesses in protecting their information and information systems due to ineffective implementation of security policies and practices."** – *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices,* GAO-17-549
- **"The Office of Personnel Management (OPM) had not fully implemented controls to address deficiencies identified as a result of a cyber incident."** - *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed,* GAO-17-614



GAO

Challenge #3: Protecting Cyber Critical Infrastructure

- The federal government has been challenged in working with the private sector to protect critical infrastructure.
- This infrastructure includes both public and private systems vital to national security and other efforts, such as providing the essential services that underpin American society.
- As the cybersecurity threat to these systems continues to grow, federal agencies have millions of sensitive records that must be protected.
- This critical infrastructure threat could have national security implications and more efforts should be made to ensure that it is not breached.

Challenge #3: Protecting Cyber Critical Infrastructure

- **"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."** *- Critical Infrastructure Protection: Additional Actions are Essential for Assessing Cybersecurity Framework Adoption,* GAO-18-211
- **"The federal government had identified major challenges to the adoption of the cybersecurity framework."** *- Critical Infrastructure Protection: Additional Actions are Essential for Assessing Cybersecurity Framework Adoption,* GAO-18-211
- **"Agencies had not addressed risks to their systems and the information they maintain."** *- Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft*, GAO-18-177
- **"Major challenges existed to securing the electricity grid against cyber threats."** *- Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention,* GAO-16-174

Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).

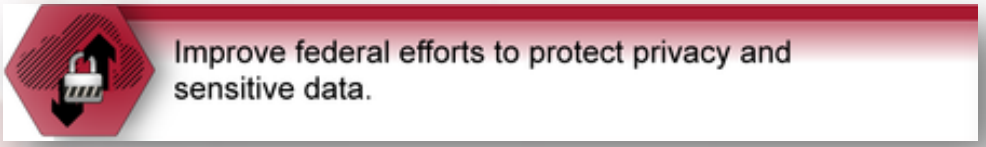
GAO

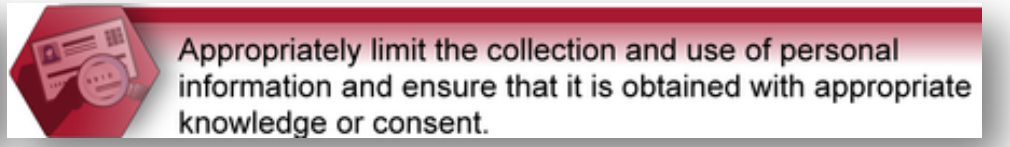
Challenge #4: Protecting Privacy and Sensitive Data

- Advances in technology, including powerful search technology and data analytics software, have made it easy to correlate information about individuals across large and numerous databases, which have become very inexpensive to maintain.
- Ubiquitous Internet connectivity has facilitated sophisticated tracking of individuals and their activities through mobile devices such as smartphones and fitness trackers.
- Given that access to data is so pervasive, personal privacy hinges on ensuring that databases of PII maintained by the government or on its behalf are protected both from inappropriate access as well as inappropriate use.
- The vast number of individuals potentially affected by data breaches at federal agencies and private sector entities in recent years increases concerns that PII is not being properly protected.

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."** – *Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement.* GAO-18-210
- **"The Equifax breach resulted in the attackers accessing personal information of at least 145.5 million individuals. "** – *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach.* GAO-18-559
- **"The emergence of IoT devices can facilitate the collection of information about individuals without their knowledge or consent"** – *Technology Assessment: Internet of Things: Status and implications of an increasingly connected world.* GAO-17-75
- **"Smartphone tracking apps can present serious safety and privacy risks."** - *Smartphone Data: Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking.* GAO-16-317





GAO

National Cyber Strategy Overview (released September 2018)

Outlines how the administration plans to:

1. Defend the homeland by **protecting networks, systems, functions, and data**;
2. Promote American prosperity by **nurturing a secure, thriving digital economy and fostering strong domestic innovation**;
3. Preserve peace and security by strengthening the United States' ability — in concert with allies and partners — to **deter and if necessary punish those who use cyber tools for malicious purposes**; and
4. **Expand American influence** abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet.

National Cyber Strategy Overview (cont.)

Lays out ten objectives that the administration plans to accomplish through 42 priority actions:

1. **Secure Federal Networks and Information** (e.g., further centralize management and oversight of federal civilian cybersecurity, improve federal supply chain risk management).
2. **Secure Critical Infrastructure** (e.g., clarify cybersecurity-related roles and responsibilities, prioritize actions according to identified national risks, incentivize cybersecurity investment, prioritize R&D).
3. **Combat Cybercrime and Improve Incident Reporting** (e.g., modernize electronic surveillance and computer crime laws, strengthen partner nations' capacity).
4. **Foster a Vibrant and Resilient Digital Economy** (e.g., invest in next generation technology).
5. **Foster and Protect United States Ingenuity** (e.g., maintain a strong and balanced intellectual property protection system).
6. **Develop a Superior Cybersecurity Workforce** (e.g., expand re-skilling and educational opportunities for American workers).
7. **Enhance Cyber Stability through Norms of Responsible State Behavior** (e.g., encourage universal adherence to cyber norms).
8. **Attribute and Deter Unacceptable Behavior in Cyberspace** (e.g., lead with objective, collaborative intelligence; impose consequences).
9. **Promote an Open, Interoperable, Reliable, and Secure Internet** (e.g., coordinate with like-minded countries, industry, academia, and civil society).
10. **Build International Cyber Capacity** (e.g., enhance cyber capacity building efforts).

GAO

Other National Cyber Strategy Priority Actions

- **Incentivize an adaptable and secure technology marketplace** – work across private and civilian stakeholder groups to promote best practices and develop strategies to overcome barriers to adoption of secure technologies; improve awareness and transparency of cybersecurity practices to build market demand for securer products/services.
- **Promote a multi-stakeholder model of Internet governance** – transparent, bottom-up, consensus-driven process for governance to ensure open, interoperable nature of the Internet in multilateral and international fora.
- **Improve space cybersecurity** – enhance efforts to protect space assets and support infrastructure from evolving cyber threats; work with industry and international partners to strengthen cyber resilience of existing/future space systems.

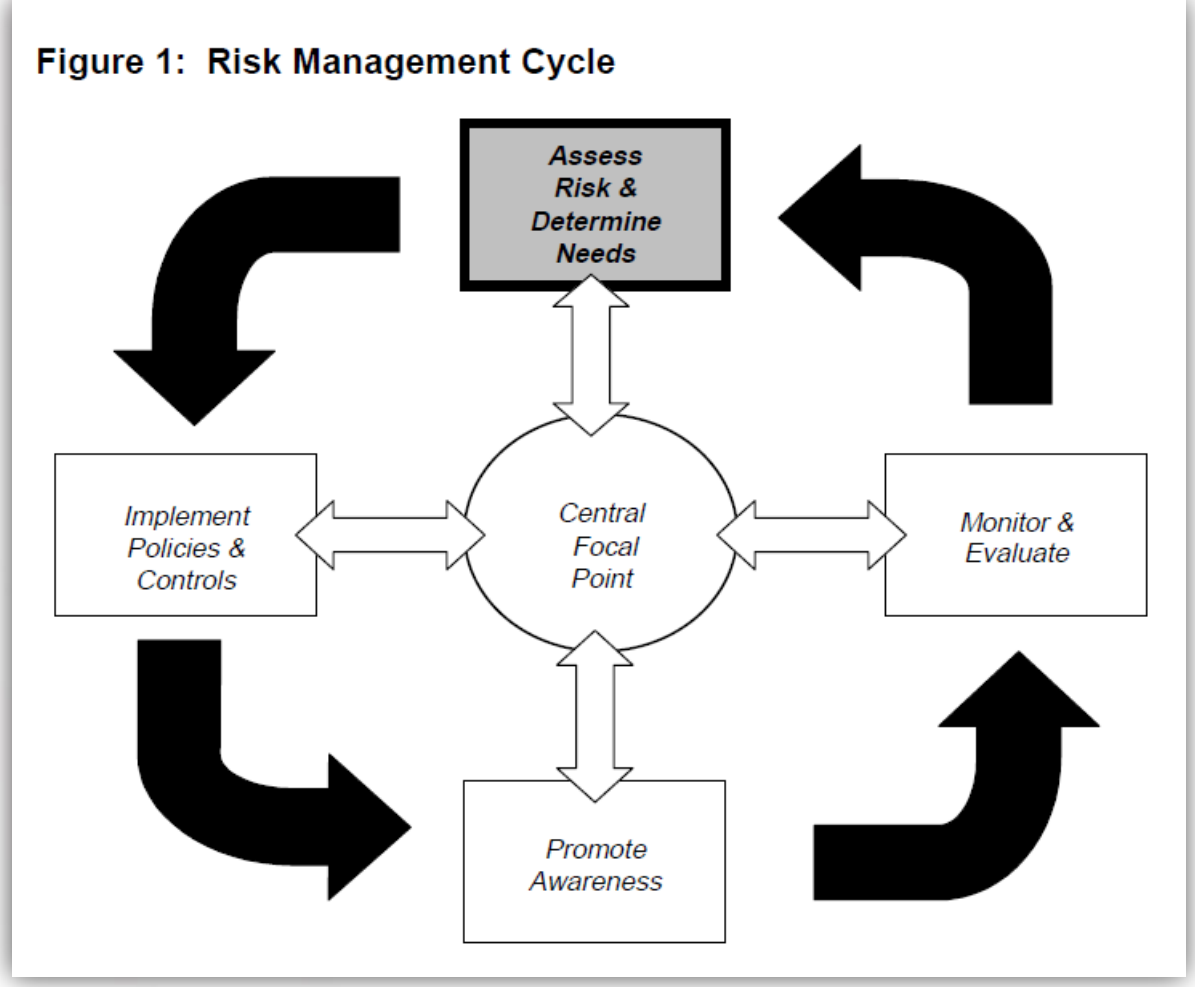
Cybersecurity is much more than just a technology fix—rather it is a risk management issue. When we focus exclusively on the technology we sometimes miss the real goal, which is managing the risk to the confidentiality, integrity and availability of the information the technology supports.

- Gen. Gregory Touhill, U.S. Chief Information Security Officer, Office of Management and Budget, in a November 2016 CIO.gov blog post

How GAO Scopes Cybersecurity and Privacy Audits

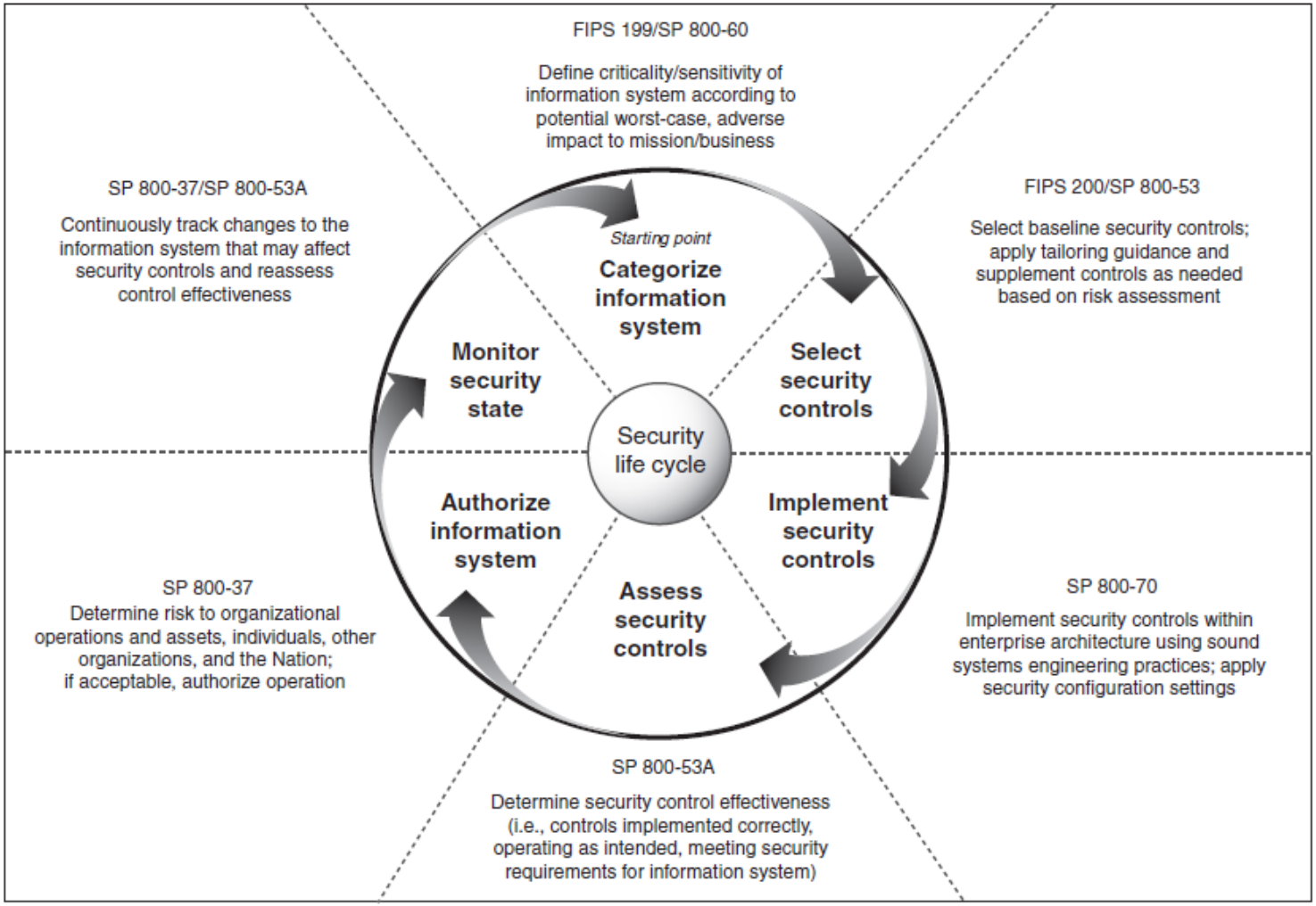
- Frameworks for selecting audit work
  - NIST Cybersecurity Framework
  - NIST 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems
  - Cybersecurity Best Practices
- Risk-based selection
  - Review prior agency reports (FISMA, IG, Financial, etc.)
  - Review significant information security incidents
  - Review third party assessments (Agency contracted work, legislatively mandated efforts, etc.)

Risk Management – Here's a Timeless Graphic



Source: Information Security Risk Assessment Practices | GAO/AIMD-00-33

NIST Risk Management Framework



Source: GAO analysis of NIST Data | GAO-10-916

NIST Cybersecurity Framework

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Source: NIST

Ongoing Work

- Ongoing
  - Cybersecurity of the Electricity Grid
  - Physical and Cybersecurity of Oil & Gas Pipelines
  - Federal Cybersecurity Risk Management
  - Intrusion Detection Systems
  - Federal Reliance on Credit Reporting Agencies for Identity Proofing
  - Census 2020 IT Readiness & Cybersecurity
  - Federal Cybersecurity Workforce
  - CDC Information Security
  - Cyber Threat Indicators and Privacy
  - Impact of Federal Cybersecurity Requirements on States

Upcoming Work

- Upcoming
  - Cybersecurity Strategy and Coordination
  - NIST Cybersecurity Framework
  - Secret Service Cybersecurity
  - Cybersecurity at HHS
  - Federal Agencies and Spear Phishing
  - Supply Chain – IT and Cyber Risks
  - HUD Data Protection
  - Binding Operational Directives
  - 5G
  - Some additional thoughts…

Challenges in Evaluating Cybersecurity

1. Challenge: Obtaining timely access to people, systems, and information
    - Agency use of audit liaison personnel
    - Agency reliance on contractors
    - Sensitivity of data
- **GAO's response:** setting expectations at entrance conferences, dual communications, escalation protocols, involvement of agency contracting technical representative, security controls over agency data, data sensitivity reviews, and separate reporting suitable for public release

2. Challenge: Hiring, developing, and retaining auditors with cyber skills
    - Demand exceeds supply
- **GAO's response:** recruiting alliances with universities, internships, career path, professional development programs, work/life balance initiatives

The Questions That Keep Coming Up on the Audit Trail

- Does the agency know its IT environment?
- Are security and privacy risks routinely and inclusively assessed by the agency?
- Are tests of the effectiveness of automated security protections performed?
- Is information on known weaknesses and vulnerabilities shared with agency leadership?

GAO

Emerging Issues

- Governing big data in the private sector
  - e.g., credit reporting agencies, information resellers, etc.
- Technology advancements too fast to regulate
  - e.g., self driving cars, smart technology, etc.
- Impact of data breaches on identity proofing
  - e.g., lose the data, spoil its use for verifying identity

GAO

Emerging Issues

- Threats to our identity beyond ID theft
  - i.e., what can lots of data and computing power be used for?
- Cyber threats to our nation
  - e.g., electric grid, financial services, and other key infrastructure

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