Cybersecurity: Securing Financial Data & The Financial Services Sector

Jennifer R. Franks, Director

Information Technology & Cybersecurity
U.S. Government Accountability Office
FranksJ@gao.gov

October 2022

Discussion Outline

- GAO Mission
- GAO High-Risk List
- The Critical Infrastructure and the Financial Services Sector
- Cyber Risks Identified By the Financial Services Sector
- Cyber Threats Faced By the Financial Services Sector
- Federal Policy and Coordination
- Securing Data & Practicing Good Cyber Hygiene
- Financial Services Sector Collaboration
- GAO Cybersecurity Recommendations

Our 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 High-Risk List

In 1990, GAO began a program to report on government operations that we identified as "high risk."

Since then, generally coinciding with the start of each new Congress, we have reported on the status of progress to address high risk areas and update the High Risk List.

1997: Cybersecurity Added to High Risk List

- When introducing information security to the High Risk list in 1997, we pointed out several related problems that needed to be addressed to help ensure that federal agencies adequately protected their systems and data:
  - Insufficient awareness and understanding of information security risks among senior agency officials
  - Poorly designed and implemented security programs that do not adequately monitor controls or proactively address risk
  - A shortage of personnel with the training and technical expertise needed to manage security controls in the sophisticated information technology environment

2003: High Risk Area Expands to Include Critical Infrastructure Cybersecurity

- In our 2003 high-risk update report, we broadened the high-risk area to include critical infrastructure cybersecurity. Specifically:
  - failure to adequately protect these infrastructures could have consequences for national security, national economic security, and/or national public health and safety;
  - terrorist groups and others have stated their intentions of attacking our critical infrastructures;
  - federal influence over the private sector's management of our nation's critical infrastructures poses unique challenges; and
  - further actions on GAO's related recommendations were needed, including (1) developing a national CIP strategy, (2) improving analysis and warning capabilities, and (3) improving information sharing on threats and vulnerabilities.

2018: High Risk Area Emphasizes the Urgency of Ensuring the Cybersecurity of the Nation

- In September 2018, we updated the cybersecurity high-risk area by identifying four major cybersecurity challenges and 10 critical actions that the federal government and other entities need to take to address them.

- A key emphasis of the update on the need for the federal government to develop and execute a comprehensive national strategy and to perform effective oversight.

- **In March 2021, the cybersecurity high-risk report was updated, and reflects that these major challenges and critical actions remain across the federal government.** (Source: GAO-21-288)

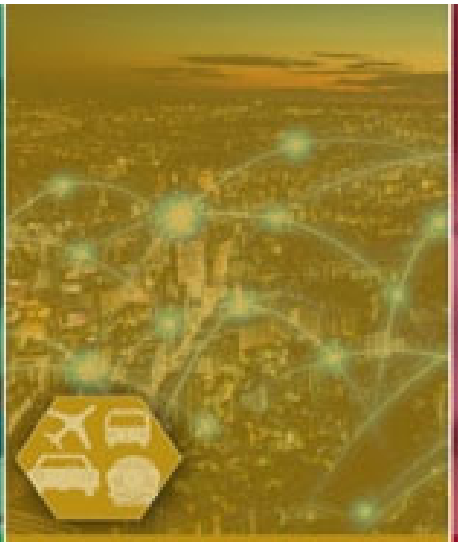
Cybersecurity High Risk Areas

Establishing a comprehensive cybersecurity strategy and performing effective oversight

1. Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.
2. Mitigate global supply chain risks (e.g., installation of malicious software or hardware).
3. Address cybersecurity workforce management challenges.
4. Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).

Securing federal systems and information

5. Improve implementation of government-wide cybersecurity initiatives.
6. Address weaknesses in federal agency information security programs.
7. Enhance the federal response to cyber incidents.

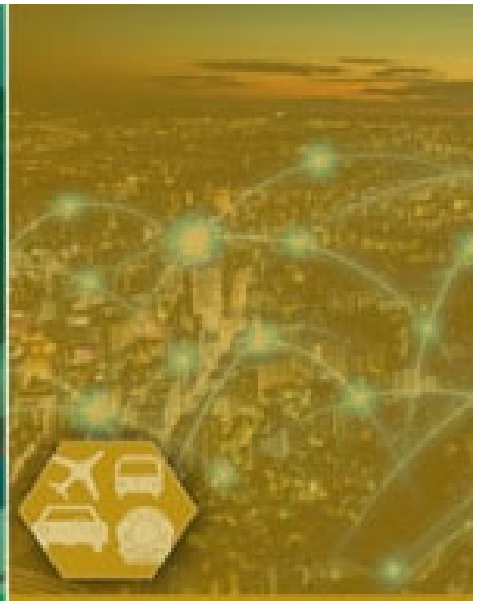


Protecting cyber critical infrastructure

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

Protecting privacy and sensitive data

9. Improve federal efforts to protect privacy and sensitive data.
10. Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.



Securing federal systems and information

5 Improve implementation of government-wide cybersecurity initiatives.

6 Address weaknesses in federal agency information security programs.

7 Enhance the federal response to cyber incidents.

Protecting cyber critical infrastructure

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

What is critical infrastructure?

- Our nation's critical infrastructure refers to the systems and assets, whether physical or virtual, so vital to the U.S. that their incapacity or destruction would have a debilitating effect on security, national economic security, economic stability, national public health or safety, or any combination of those matters.
- The U.S. has 16 critical infrastructure sectors that provide the essential services—such as banking, clean water, electricity, and oil and gas distribution—that underpin American society.
- These sectors rely on electronic systems and data to support their missions.

Critical Infrastructure Sectors -and- Related Sector Risk Management Agencies

Sector risk management agency

Departments of Agriculture (USDA), Defense (DOD), Energy (DOE), Health and Human Services (HHS), Homeland Security (DHS), Transportation (DOT), the Treasury; Environmental Protection Agency (EPA); and the General Services Administration (GSA)

Source: GAO analysis of Presidential Policy Directive-21 and DHS's National Infrastructure Protection Plan 2013; Art Explosion (clip art). | GAO-22-105103

What is the financial services sector?

- The Financial Services Sector represents a vital component of our nation's critical infrastructure.
- The sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions.

Cyber Risks Identified by Financial Sector Firms and Federal Agencies

1. Social Engineering
2. Malware
3. Third-Party Access
4. Insider Threats
5. Interconnectivity

Source: GAO-20-631

Cyber Threats Faced by the Financial Services Sector

- The attacks of September 11, 2001, caused the securities markets and several futures exchanges to close until communications and other services were transferred to alternate sites or restored to lower Manhattan.
- Beginning in the summer of 2012, financial institutions, including smaller institutions, experienced a series of coordinated distributed denial-of-service (DDoS) attacks against their public-facing websites. These incidents affected customer access to banking information, but did not impact core systems or processes.

Cyber Threats Faced by the Financial Services Sector

- On October 29, 2012, the landfall of Superstorm Sandy caused a two-day closure of major equities exchanges, while fixed income markets were closed for one day.
- In July 2017, Equifax discovered that attackers had gained unauthorized access to one of its portals used to resolve consumer disputes. The Equifax breach resulted in the attackers accessing personal information of at least 145.5 million individuals.
- In December 2021, the personal information of 1.5 million Flagstar Bank customers was affected by the hacking of the bank's systems. The Michigan-based bank operates 150 branches and is one of the country's largest mortgage lenders.

Federal Policy

- Presidential Policy Directive 21, issued in February 2013, shifted the nation's focus from protecting critical infrastructure against terrorism to protecting and securing it and increasing its resilience against all hazards, including cyberattacks.

- This directive and federal law also call for the Department of Homeland Security (DHS) to coordinate the overall federal effort to secure and protect against critical infrastructure risks.

Federal Coordination and Guidance

- **Office of the National Cyber Director**
  - Serves as the principal advisor to the White House on cybersecurity policy and strategy, including coordination of implementation of national cyber policy and strategy.
  - An important step toward positioning the federal government to better direct activities to address the nation's cyber threats.
- **NIST Cybersecurity Framework**
  - A framework of cybersecurity standards and procedures that industry can adopt.
  - Divided into four core elements: (1) identify, (2) protect, (3) detect, (4) respond, and (5) recover

DHS & CISA's Role

- The Cybersecurity and Infrastructure Security Agency (CISA), within DHS, is the lead federal agency for coordinating efforts to understand and manage risks to critical infrastructure.
- Since the passage of the *Cybersecurity and Infrastructure Security Agency Act of 2018*, CISA's National Risk Management Center has led the agency's risk-identification and analysis functions.
- The center performs risk assessments, modeling, and data management to understand crosscutting critical infrastructure risks and support policy making, process enhancements, and risk-management decisions.

Treasury's Role

- The Department of Treasury is designated as the Sector Risk Management Agency for the Financial Services Sector and is responsible for developing a sector-specific plan through a coordinated effort involving its public and private sector partners.
- The Financial Services Sector-Specific Plan (SSP) provides an overview of the sector and the cybersecurity and physical risks it faces, establishes a strategic framework that serves as a guide for prioritizing the sector's day-to-day work, and describes the key mechanisms through which the strategic framework is implemented and assessed.

GAO

Understanding Cyber Risks:
Securing Data & Practicing Good Cyber Hygiene

- Require multi-factor authentication
- Employ least privileged principle
- Delegate permissions to roles rather than people
- Implement strong access controls
- Perform threat intelligence and risk assessments
- Conduct regular vulnerability scanning and analyses
- Update incident detection, response, and recovery capabilities
- Perform continuous monitoring
- Provide adequate security awareness and role-based training

Collaboration Is Key!

- Outcomes and accountability
- Bridging organizational cultures
- Clarity of roles and responsibilities
- Leadership
- Participants
- Resources
- Written guidance and agreements
- Source: GAO-21-403

Financial Services Sector Collaboration

In response to the cybersecurity and physical risks faced by the sector, numerous critical infrastructure partners collaborate on multiple levels to enable the sector's security and resilience.

These partners include:

- a network of Financial Services Sector companies;
- sector trade associations;
- federal government agencies;
- financial regulators;
- state, local, tribal, and territorial governments; and
- other government and private sector partners in the U.S. and around the world.

GAO Cybersecurity Recommendations

- Since 2010, GAO has made over 3,800 recommendations to federal agencies to address cybersecurity shortcomings—and we reported that more than 820 of these had not been fully implemented as of June 2022.
- Of these more than 820 recommendations, we designated 116 as priority recommendations, meaning that we believe these recommendations warrant priority attention from heads of key departments and agencies. However, as of June 2022, 44 of these priority recommendations had not been fully implemented.

GAO on the Web

Connect with GAO on LinkedIn, Facebook, Flickr, Twitter, YouTube and our Web site: https://www.gao.gov/
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts and read The Watchblog

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@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

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov,
(202) 512-4707, U.S. Government Accountability Office,
441 G Street NW, Room 7814, Washington, DC 20548

Copyright