Auditing Cybersecurity Through Risk Management

New England Intergovernmental Audit Forum Meeting

Nick Marinos
Director, Information Technology Team
U.S. Government Accountability Office

May 22, 2017

Agenda

- About GAO
- Current State of Cybersecurity in the Federal Government
- Risk-based Approaches to Evaluate the Effectiveness of Cybersecurity Processes and Controls
- Case Study 1: Air Traffic Controls Systems Security
- Case Study 2: High Impact System Security
- Challenges and Observations from the Audit Trail

About GAO: Our Mission

To support the U.S. 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 the U.S. Congress with timely information that is* ***objective, fact-based, nonpartisan, nonideological, fair, and balanced****.*

About GAO: Our Work

- Part of the legislative branch
- Headed by the Comptroller General (CG)
- Receive requests and mandates from the U.S. Congress
- CG Authority: can self-initiate work

About GAO: Audit Policy

Core Values	• Accountability • Integrity • Reliability
Government Auditing Standards	• Independence • Professional Judgment • Competence • Quality Control and Assurance

About the IT Team: Audit Areas

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

GAO's Work on Cybersecurity: Areas Covered

Agency Information Security

- Security programs, policies, practices, and controls
- Controls over financial systems
- Cybersecurity workforce

Emerging Issues

- Cloud computing
- Internet of Things
- Continuous diagnostics and mitigation
- Incident detection and response

Critical Infrastructure Protection

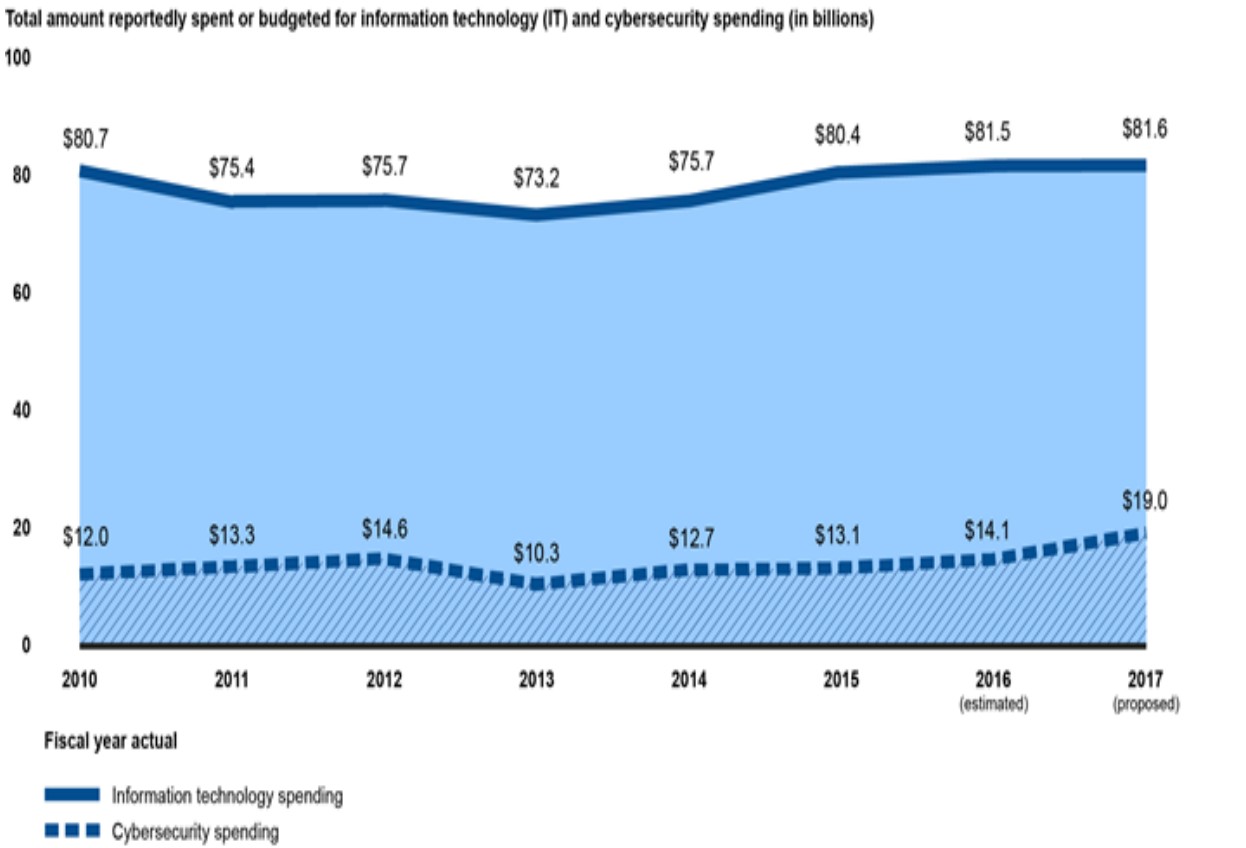
- Air traffic control systems security
- Cybersecurity framework for critical infrastructure
- Government efforts to protect privately owned cyber infrastructure

GAO's Work on Cybersecurity: It Takes a Village

INFORMATION TECHNOLOGY	ARM Applied Research and Methods	PI Physical Infrastructure
Mission Team	Stakeholder	Stakeholder
FMA FINANCIAL MANAGEMENT AND ASSURANCE	HSJ Homeland Security and Justice	DCM Defense Capabilities & Management
Stakeholder	Stakeholder	Stakeholder

Billions Spent on Federal IT and Cybersecurity

- U.S. government annually spent between:
  - $73.2 and $80.7 billion on IT
  - $10.3 billion and $14.6 billion on IT security activities.
- Defense spending dwarfs other agencies.
- Civilian agencies reportedly spent about 8 percent of IT budget on security in FY 15.
- IT security spending for FY 17 was proposed last year for a 35 percent increase.



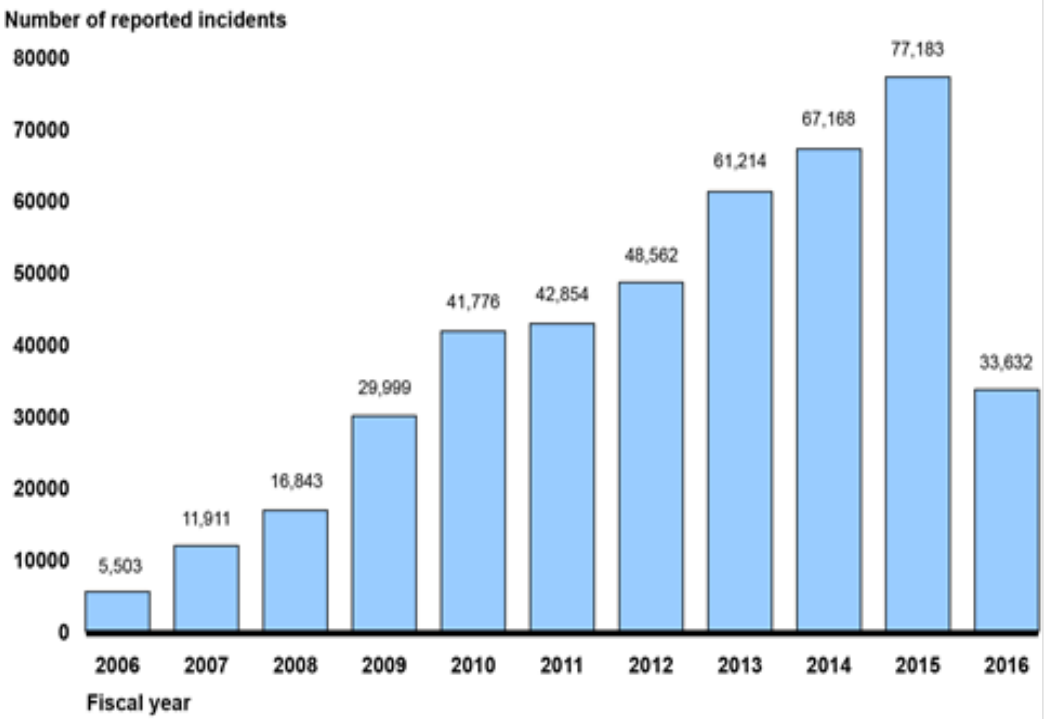
Source: GAO analysis of IT spending reports from President's budgets, Office of Management and Budget FISMA reports, and the Cybersecurity National Action Plan.

Management of IT Acquisitions and Operations: Why High Risk?

- More than $89 billion that is annually invested in information technology (IT) by the federal government
- Federal IT investments too frequently fail or incur cost overruns and schedule slippages while contributing little to mission-related outcomes.
- Legacy systems exist across the federal government that agencies report are 30 years or older and use obsolete software or hardware and do not have specific plans with time frames to modernize or replace these investments

Cybersecurity and the Federal Government: Why High Risk?

- From fiscal year 2006 through 2015, reported security incidents increased about 1,300 percent.
- Increases likely due to:
  - Better reporting
  - Better detection
  - Active threats
  - Vulnerable systems
- Steep drop in incidents reported in fiscal year 2016 likely due to changes in reporting requirements.

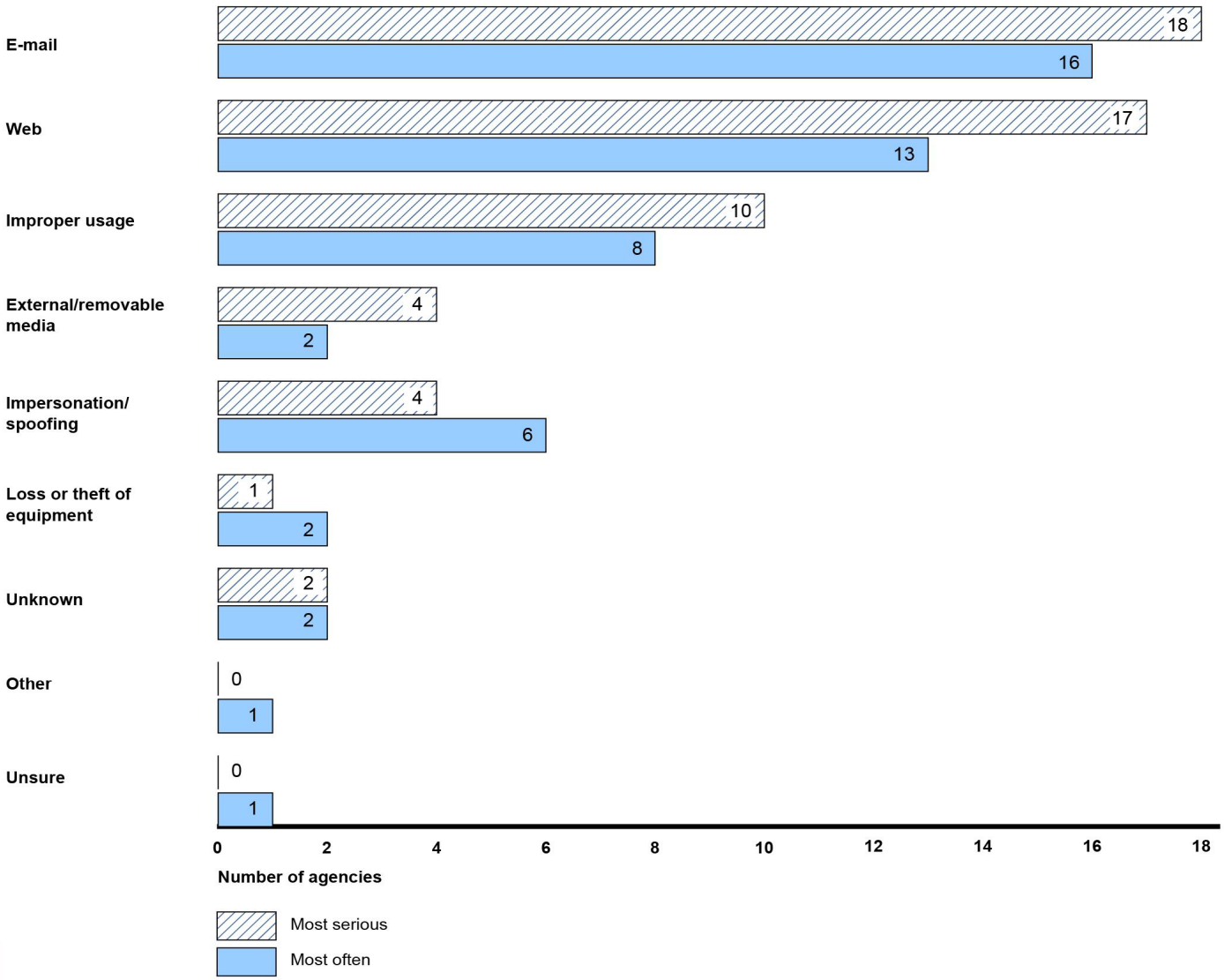


Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2016.

Vectors Used to Attack IT Systems

- Federal agencies identified **email and websites** as the most serious and frequent threat vectors that affect their systems.

Most Serious and Most Frequently Identified Cyber Threat Vectors, as Reported by Agencies

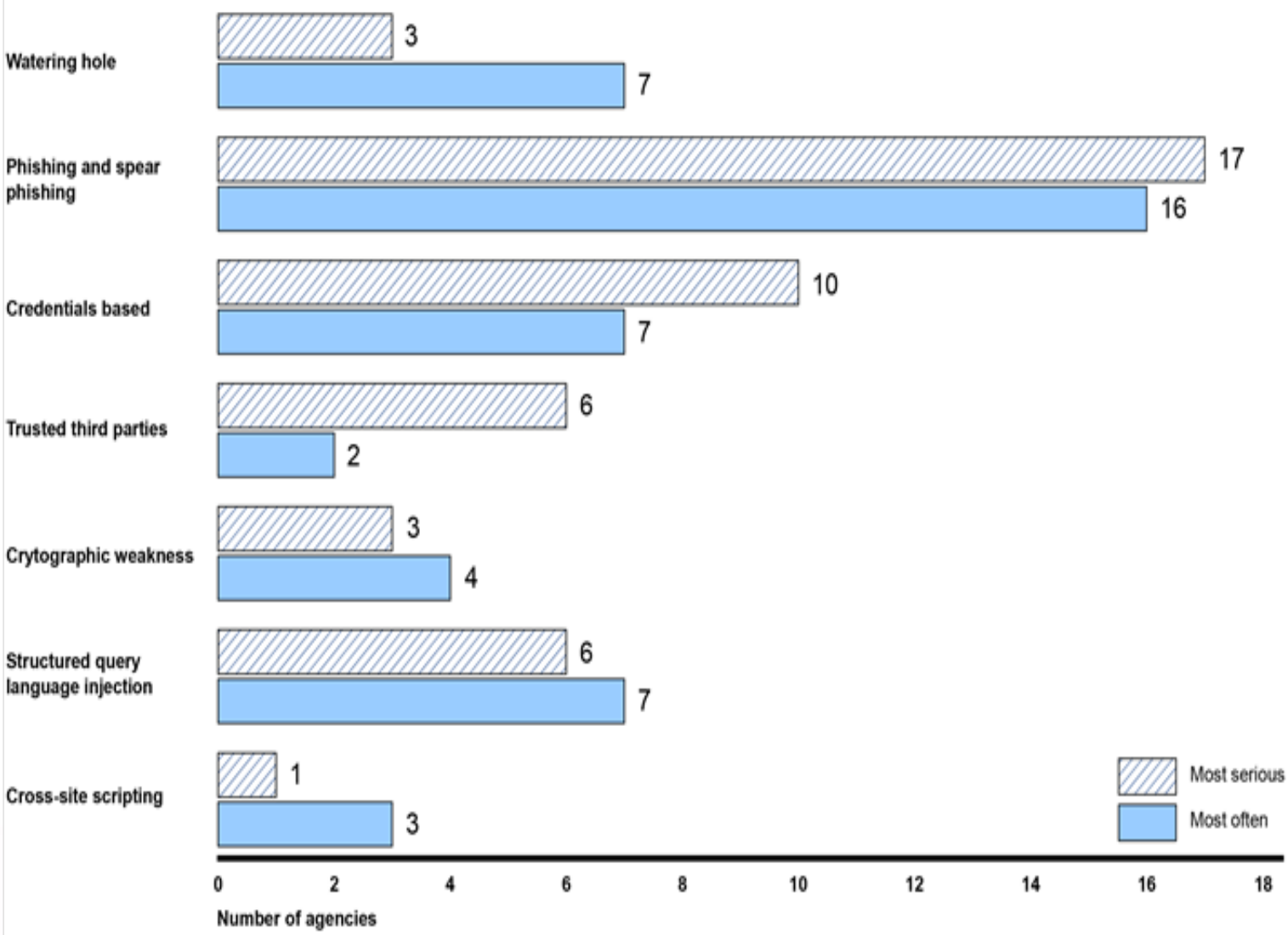


Source: GAO summary based on responses to GAO survey. | GAO-16-501

Techniques Used to Attack IT Systems

- **Phishing** and exploiting **credentials** vulnerabilities were the most serious and frequent techniques used.

Most Serious and Most Frequently Identified Attack Techniques, as Reported by Agencies



Source: GAO summary based on responses to GAO survey. | GAO-16-501

Federal Requirements in Law

- Federal Information Security Management Act of 2002 (amended in 2014)
  - Outlines the elements of an information security program
  - Assigns responsibility for the implementation of the security and privacy program
  - Creates reporting requirements for breaches
- Privacy Act of 1974 and E-Gov Act of 2002
  - Outlines the principles for protecting the privacy of individuals' personally identifiable information

How Agencies Design their Information Security and Privacy Programs

- Federal Law (FISMA / Privacy Act / E-Gov Act / etc.)

- OMB Memoranda and Circulars
  - OMB Circular A-123
    "Management's Responsibility for Enterprise Risk Management and Internal Control"
  - OMB Circular A-130
    "Managing Information as a Strategic Resource"

- NIST Guidance
  - NIST SP 800-53
  - NIST Risk Management Framework
  - NIST Cybersecurity Framework

OMB Circular A-123 & Risk Management

Prior to this revision, A-123 focused on internal control largely in the context of financial management. The revision is intended to shift to a much broader vision of enterprise-wide risk management as a means of managing agency mission and business activities.

A-123's major requirements for agencies are:

- Establish goals and objectives around operating environments in order to ensure compliance with laws and regulations, and manage both expected and unexpected events;
- Implement management practices that identify, assess, respond, and report on risk; and
- Establish and maintain internal controls to achieve control objectives related to operations, reporting, and compliance.

OMB Circular A-123 & Risk Management

- OMB Circular A-123 (revised 2016)
  - The new A-123 requires agencies to implement an Enterprise Risk Management (ERM) capability coordinated with GPRAMA strategic planning and review, and the internal control processes required by FMFIA and GAO's Green Book.
  - According to A-123, "ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that provide better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery."

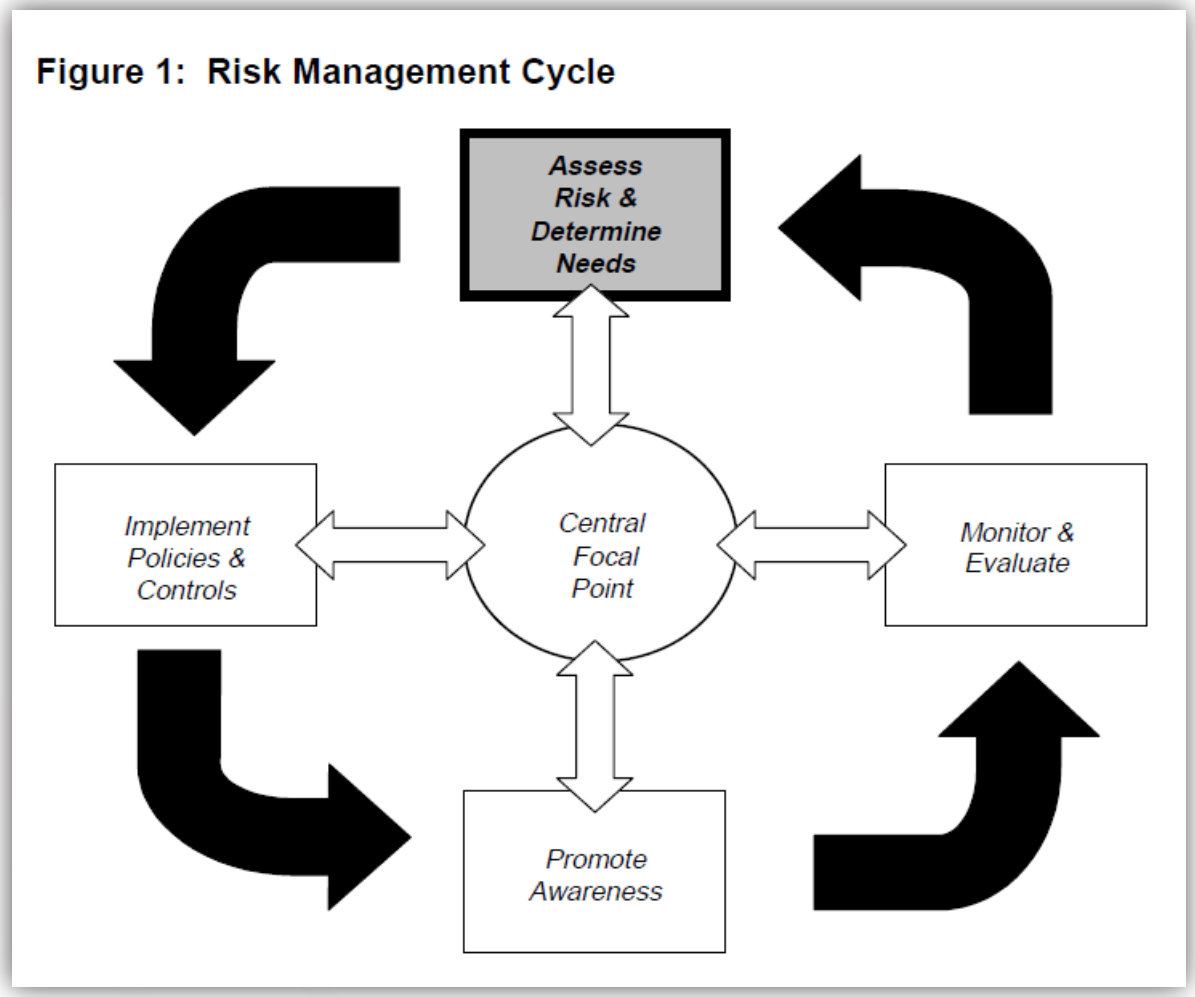
OMB Circular A-130 & Risk Management

- OMB Circular A-130 (revised 2016)
  - Appendix I gives agencies a broad definition of risk management activities including the NIST Risk Management Framework:
    - "The Risk Management Framework, as described in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities in the system development life cycle."
    - An effective implementation of the Risk Management Framework ensures that managing information system-related risks is consistent with the agency's mission or business objectives and overall risk management strategy, and risk tolerance established by the senior leadership through the risk executive function."
  - One of its reported purposes is to link agency information security programs and agency management control systems established in accordance with Circular A-123.

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.

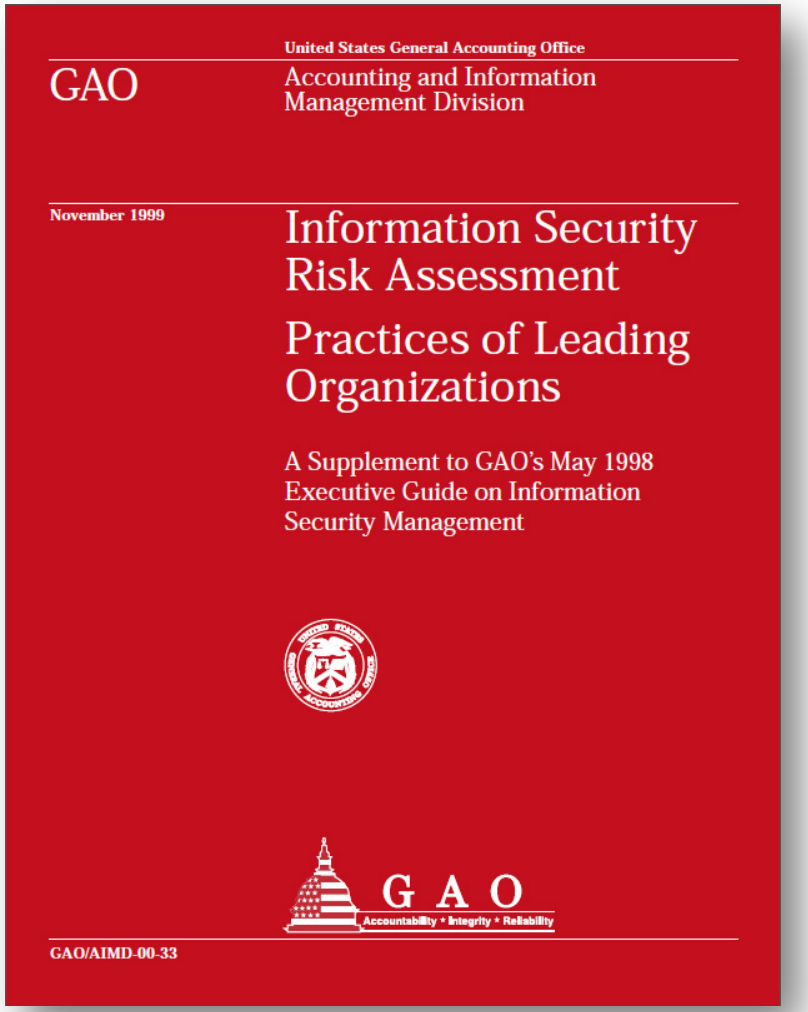
- Gen. Gregory Touhill, U.S. Chief Information Security Officer, Office of Management and Budget, in a November 2016 CIO.gov blog post

Risk Management – Here's a Timeless Graphic



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

Risk Management – Circa 1999

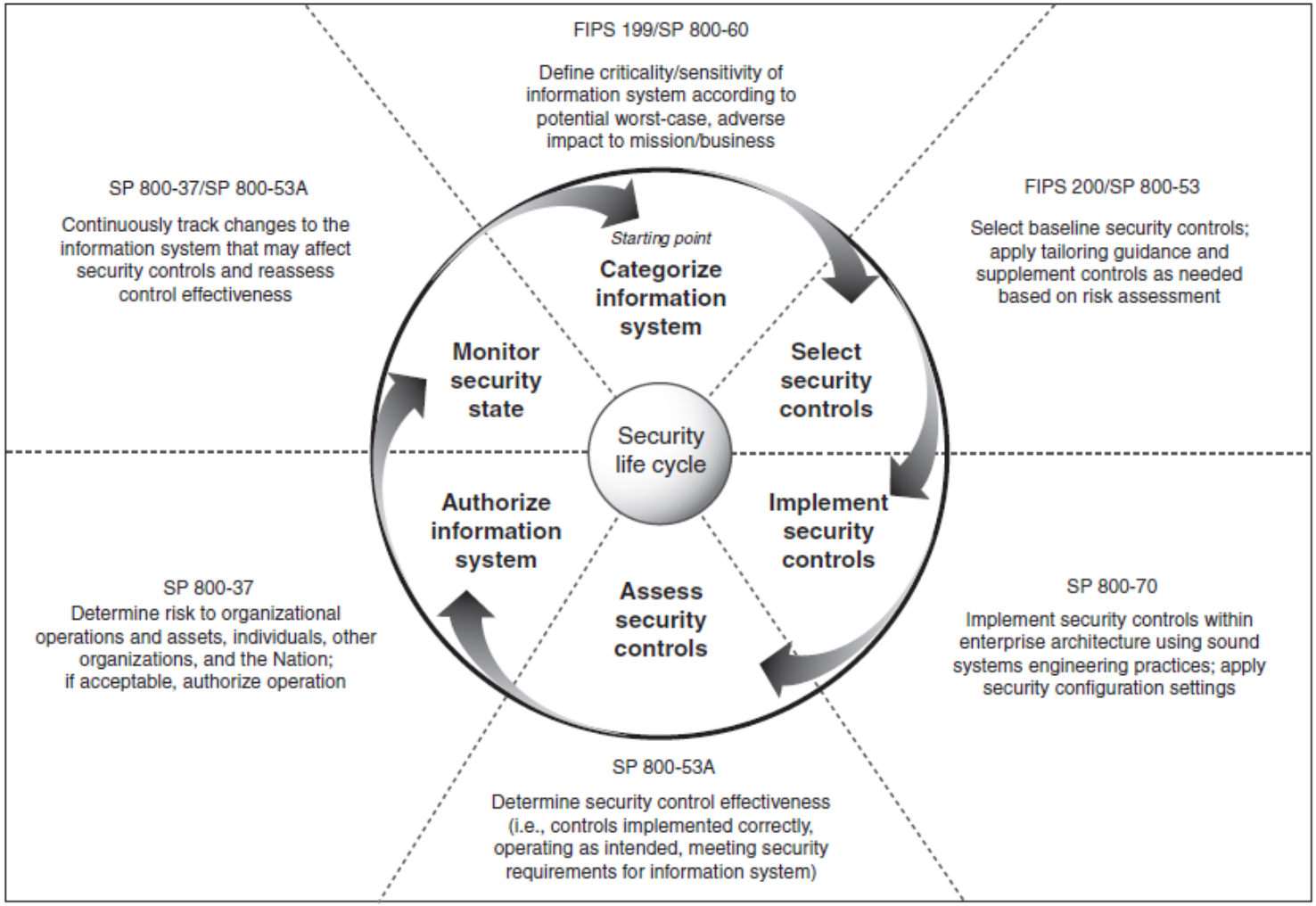


Source: Information Security Risk Assessment Practices | GAO/AIMD-00-33

Critical Success Factors for Risk Management

- Obtain senior management support and involvement
  - *What's the role of the CIO and CISO organizations and when do they get involved?*
- Designate focal points
- Define procedures
- Involve business and technical experts
  - *Are all the right parties at the table?*
- Hold business units responsible

NIST Risk Management Framework



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

NIST Cybersecurity Framework

https://www.nist.gov/cyberframework

NIST Cybersecurity Framework

Special Publication 800-39			Cybersecurity Framework Components
	Level 1 Organization	**Integrate enterprise and cybersecurity risk management** by communicating with universally understood risk terms.	Core
	Level 2 Mission/ Business Processes	**Manage cybersecurity requirements** using a construct that enables integration and prioritization of *all* requirements.	Profile(s)
		Integrate and align cybersecurity and acquisition processes by relaying cybersecurity requirements and priorities in a common and concise language	Profile(s)
		Evaluate organizational cybersecurity using a standardized and straightforward measurement scale and set of self-assessment criteria.	Implementation Tiers
		Manage the cybersecurity program by determining which cybersecurity outcomes necessitate common controls, and apportioning work and responsibility for those cybersecurity outcomes (supports RMF Implement & Monitor).	Profile(s)
		Maintain a comprehensive understanding of cybersecurity risk using a standardized organizing structure (supports RMF Authorize).	Core
		Report cybersecurity risks using a universal and understandable reporting structure.	Core
	Level 3 System	**Inform the tailoring process** using a comprehensive reconciliation of *all* cybersecurity requirements (supports RMF Implement).	Profile(s)

Source: National Institute of Standards and Technology

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

GAO's Work on Cybersecurity

- Reviewing the effectiveness of cybersecurity at federal agencies to better ensure the protection of government and personal information.

- Evaluating federal efforts to enhance the cybersecurity of private- and public-sector computer information systems and networks vital to operating U.S. critical infrastructure.

How GAO Scopes Security and Privacy Audits

- Frameworks for selecting audit work
  - Federal Information System Controls Audit Manual (FISCAM)
  - NIST Cybersecurity Framework
  - NIST 800-37
    Guide for Applying the Risk Management Framework to Federal Information Systems
- 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.)

How GAO Performs Security and Privacy Audits

- Criteria
  - Federal Information Processing Standards (FIPS)
  - Special Publications
  - NIST Internal or Interagency Reports (NISTIRs)
  - Vendor best practices
    - National Checklist Program (NCP)
    - Configuration guidance from vendors

How GAO Examines Agency IT Security Processes

- Assessing cyber risks
- Selecting and documenting IT security controls
- Providing security training
- Monitoring, testing, and evaluating controls
- Detecting, responding, and recovering from incidents
- Mitigating vulnerabilities
- Overseeing contractors

Results of GAO Audits

- Identified information security as high-risk area since 1999.
- Recommended improvements including the need to:
  - Effectively implement risk-based information security programs.
  - Improve capabilities for detecting, responding to, and mitigating cyber incidents.
  - Expand cyber workforce and training efforts.
- GAO reports on IT security have led to:
  - Greater awareness of cybersecurity and privacy risks to the federal government, critical infrastructure, and public.
  - An improved federal cybersecurity strategy.
  - Stronger information security programs and controls at U.S. government agencies.
  - Improved legislation on cybersecurity.

Typical GAO Recommendations

- Change vendor-supplied IDs and passwords
- Strengthen authentication controls
- Restrict administrator privileges based on user duties
- Remove inactive accounts & accounts of separated users
- Patch applications and operating systems timely
- Keep software current
- Use encrypted protocols
- Apply access control lists

Typical GAO Recommendations

- Provide role-based training for those with significant security responsibilities
- Establish & deploy secure configurations for HW & SW
- Monitor assets, configurations, vulnerabilities frequently
- Test effectiveness of IT security controls
- Remedy known vulnerabilities timely
- Verify effectiveness of remediation efforts
- Implement adequate incident detection and response
- Test viability of contingency plans and back-up procedures

Case 1: Air Traffic Control Systems Security

Background

- The U. S. Federal Aviation Administration (**FAA**) performs critical functions that contribute to ensuring safe, orderly, and efficient air travel in the airspace above and approaching the United States.
- One such function, maintaining effective air traffic control (**ATC**), relies on automated systems to provide information to air traffic controllers and aircraft flight crews to work toward ensuring safe and expeditious movement of aircraft.

Case 1: Air Traffic Control Systems Security

Background

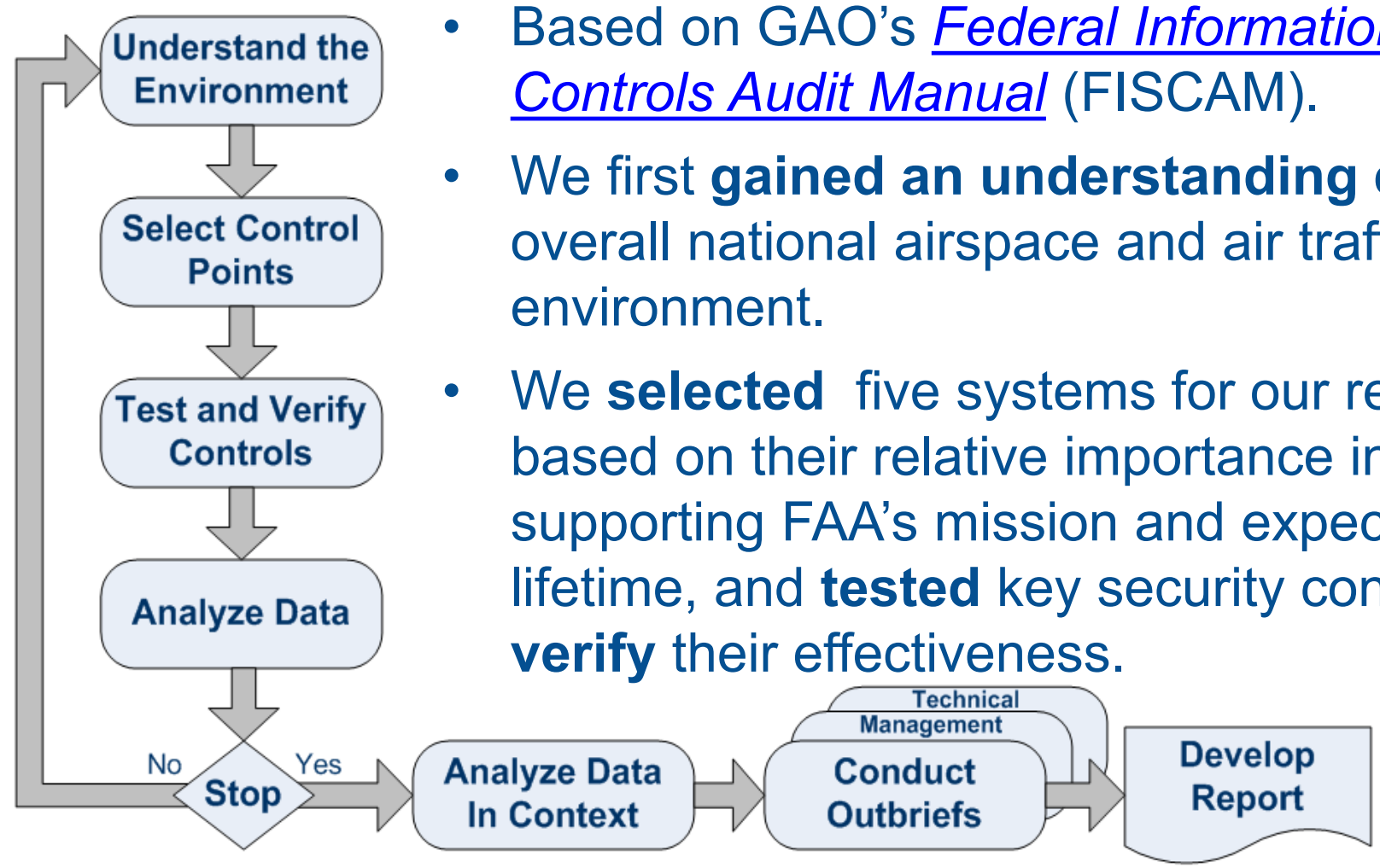
- New networking technologies connecting FAA's systems expose them to new cybersecurity risks, which increase opportunities for systems to be compromised or damaged.

Summary of Air Traffic Control over the U.S.

Source: GAO based on Federal Aviation Administration information. | GAO-15-221

Case 1: Air Traffic Control Systems Security

Scope & Methodology



- Based on GAO's *Federal Information System Controls Audit Manual* (FISCAM).
- We first **gained an understanding** of the overall national airspace and air traffic control environment.
- We **selected** five systems for our review based on their relative importance in supporting FAA's mission and expected lifetime, and **tested** key security controls to **verify** their effectiveness.

Case 1: Air Traffic Control Systems Security

What We Found

- FAA had **taken steps to safeguard** its air traffic control systems by, for example, establishing related policies and procedures and implementing key protections.
- ATC systems and networks were riddled with **significant security control weaknesses**.
- A key reason for these weaknesses was the lack of an integrated, **organization-wide approach** to managing information security risk.

Case 1: Air Traffic Control Systems Security

We made:

- 17 recommendations to FAA to fully implement its information security program and establish an integrated approach to managing information security risk.
- 168 recommendations to strengthen access controls and configuration management of ATC systems.

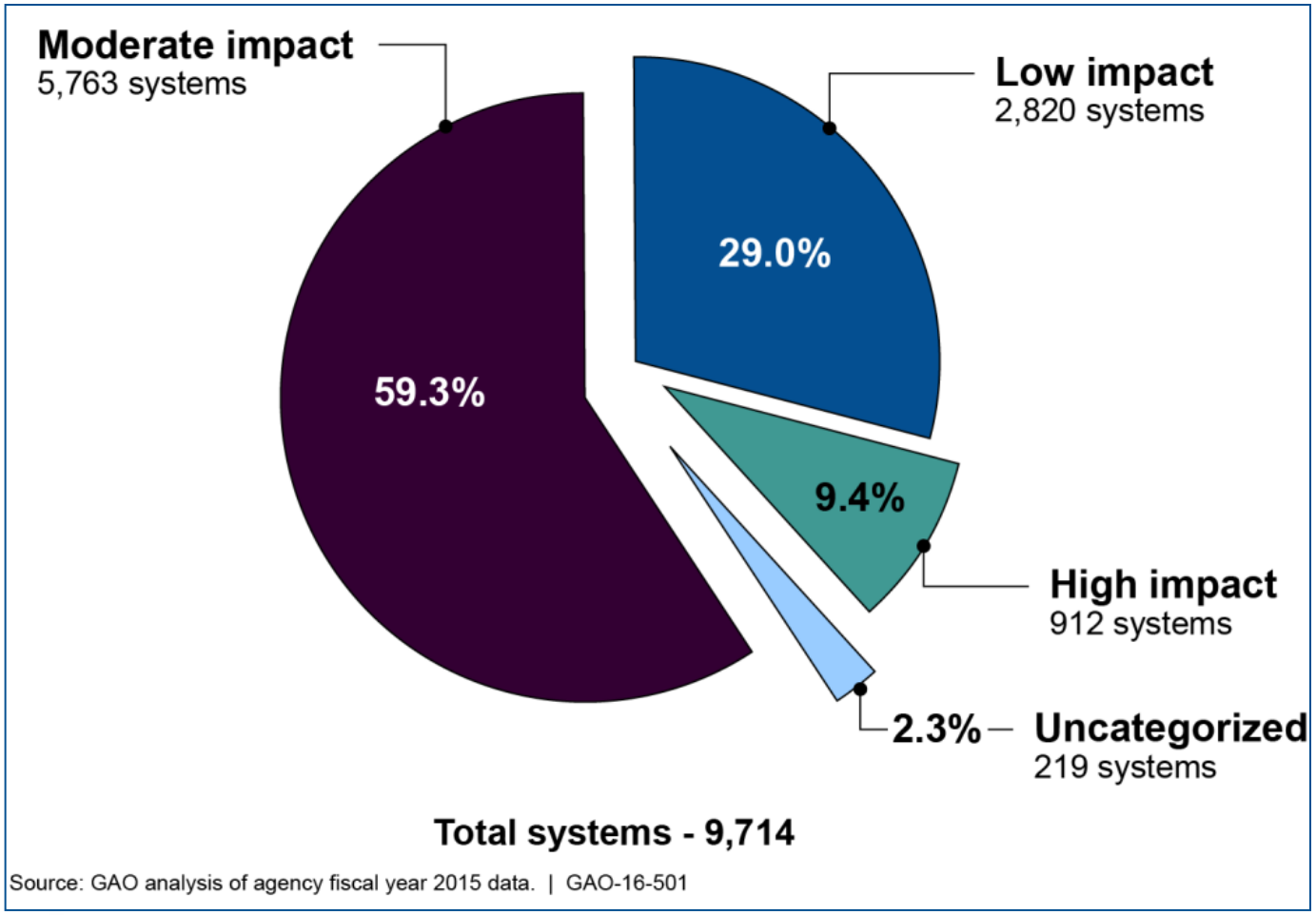
FAA concurred with all of our recommendations and stated that it has taken, or plans to take, actions to address them.

Case 2: Security of High Impact Systems

Federal systems are categorized based on the potential impact of the loss of confidentiality, integrity, or availability of information they contain:

- Low Impact: **limited** adverse effect
- Moderate Impact: **serious** adverse effect
- High Impact: **severe or catastrophic** adverse effect

Categorization of Impact Level for Federal Systems in FY 2015



Source: GAO analysis of agency fiscal year 2015 data. | GAO-16-501

Case 2: Security of High Impact Systems

Audit Scope and Methodology

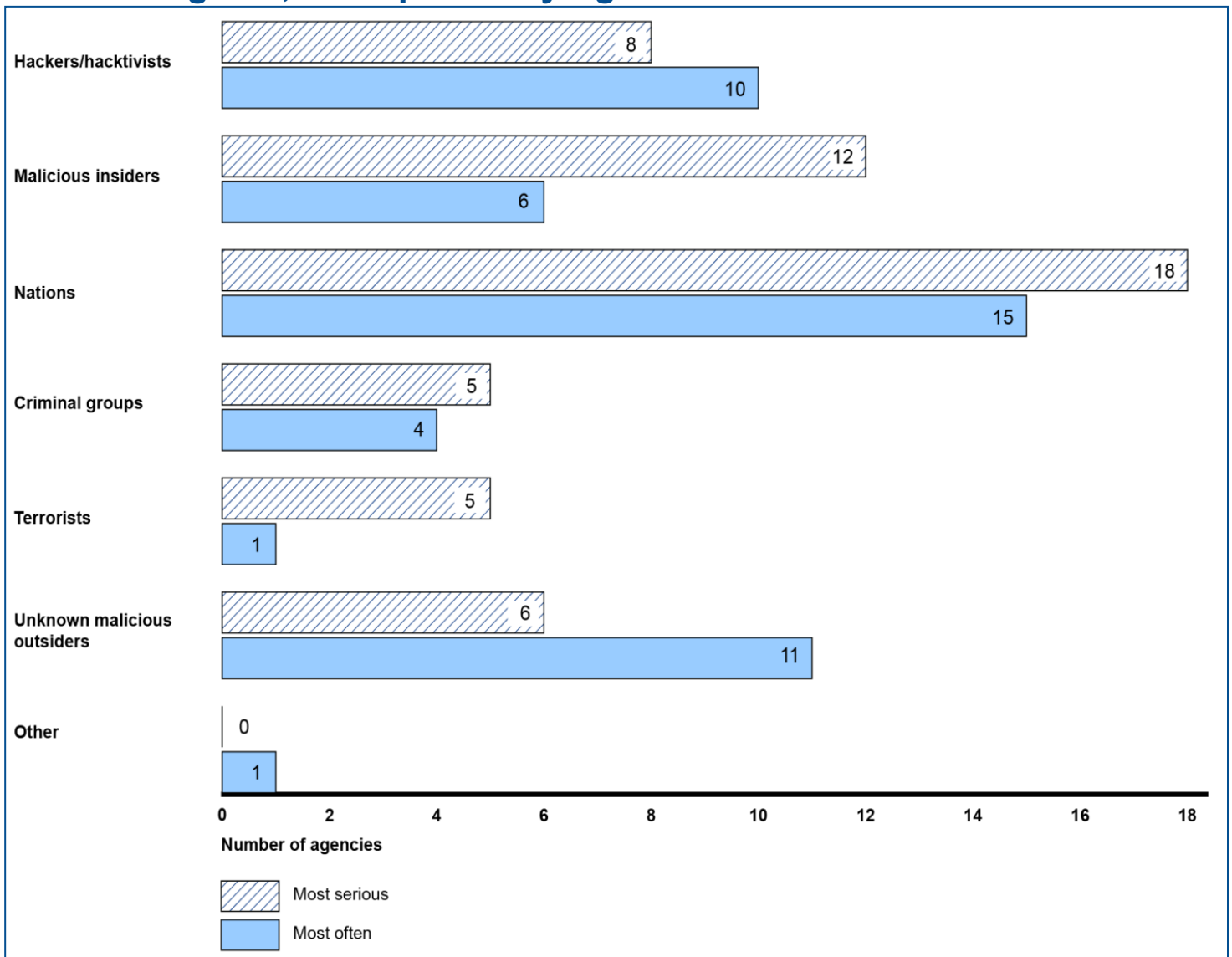
- **Surveyed** 24 major federal agencies to collect, analyze, and summarize data on the cyber threats, security incidents, and security guidance and efforts involving high-impact systems.
- **Examined** federal policies, standards, guidelines, reports by organizations with government-wide information security responsibilities.
- **Interviewed** officials at these organizations about guidance and services to protect federal systems.
- **Tested** security controls over 8 high-impact systems at 4 agencies.

Case 2: Security of High Impact Systems

What We Found:

- Federal agencies identified **cyber attacks from nations** as the most serious and frequent threat to the security of their systems.

Most Serious and Most Frequently Identified Adversarial Cyber Threat Sources/Agents, as Reported by Agencies



Source: GAO summary based on responses to GAO survey. | GAO-16-501

Case 2: Security of High Impact Systems

What We Found (continued):

- The 4 selected agencies had implemented numerous controls over the 8 high-impact systems we reviewed. For example, each of the agencies reviewed had developed a **risk assessment** for the selected high-risk systems.
- However, the 4 agencies had not effectively implemented **patch management, contingency planning,** and **access controls** such as identifying and authenticating users, authorizing access needed to perform job duties, and auditing and monitoring system activities.

Case 2: Security of High Impact Systems

We made:

- 2 recommendations to an oversight agency to complete its plans and practices for securing federal systems.
- 19 recommendations to the four selected agencies related to fully implementing key elements of their security programs.
- 261 additional recommendations to the four agencies to mitigate identified vulnerabilities in access controls, patch management, and contingency planning.

The agencies generally concurred with most of our recommendations, although 3 agencies did not concur with 41 recommendations.

Our Challenges in Evaluating IT Security

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 Reports on IT Systems Security in FY 2016

- GAO-16-885T, *Federal Information Security: Actions Needed to Address Challenges* (September 2016)
- GAO-16-771, *Electronic Health Information: HHS Needs to Strengthen Security and Privacy Guidance and Oversight* (August 2016)
- GAO-16-691SU, *Information Security: VA Needs to Improve Controls over Selected High-Impact Systems (September 2016)*
- GAO-16-689SU, *Information Security: NRC Needs to Improve Controls over Selected High-Impact Systems* (August 2016)
- GAO-16-688SU, *Information Security: NASA Needs to Improve Controls over Selected High-Impact Systems (September 2016)*
- GAO-16-687SU, *Information Security: OPM Needs to Improve Controls over Selected High-Impact Systems* (August 2016)
- GAO-16-686, *Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority* (August 2016)
- GAO-16-605, *FDIC Implemented Controls Over Financial Systems, but Further Improvements are Needed* (June 2016)
- GAO-16-604SU, *FDIC Implemented Controls Over Financial Systems, but Further Improvements are Needed* (LOUO)
- GAO-16-590T, *Information Security: IRS Needs to Further Enhance Controls over Taxpayer and Financial Data* (April 2016)
- GAO-16-589T, *Information Security: IRS Needs to Further Enhance Controls over Taxpayer and Financial Data and Continue Identity Theft Refund Fraud* (April 2016)
- GAO-16-574, *Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises (September* 2016)
- GAO-16-513, *Information Security: FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk (August 2016)*
- GAO-16-512SU, *Information Security: FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk* (June 2016)
- GAO-16-501, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems (June 2016)*
- GAO-16-493, *Information Security: Opportunities Exist for SEC to Improve Its Controls over Financial Systems and Data (April 2016)*
- GAO-16-445SU, *Information Security: Opportunities Exist for SEC to Improve Its Controls over Financial Systems and Data (LOUO)*

GAO Reports on IT Systems Security in FY 2016

- GAO-16-398, *Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data (March 2016)*
- GAO-16-397SU, *Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data (LOUO)*
- GAO-16-350, *Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack (March 2016)*
- GAO-16-317, *SmartPhone Data: Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking (April 2016)*
- GAO-16-294, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System (January 2016)*
- GAO-16-265, *Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls (March 2016)*
- GAO-16-264SU, *Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls (LOUO)*
- GAO-16-228T, *Department of Education and Other Federal Agencies Need to Better Implement Controls (November 2015)*
- GAO-16-194T, *Information Security: Federal Agencies Need to Better Protect Sensitive Data (November 2015)*
- GAO-16-174T, *Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention (October 2015)*
- GAO-16-152, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework (December 2015)*
- GAO-16-116T, Maritime *Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity (October 2015)*
- GAO-16-79, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress (November 2015)*
- GAO-16-43SU, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System (LOUO)(November 2015)*

GAO on the Web

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

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.