Cybersecurity Issues and IT Security Audits

Presented to:

New York / New Jersey Intergovernmental Audit Forum Meeting

May 3, 2017

Agenda

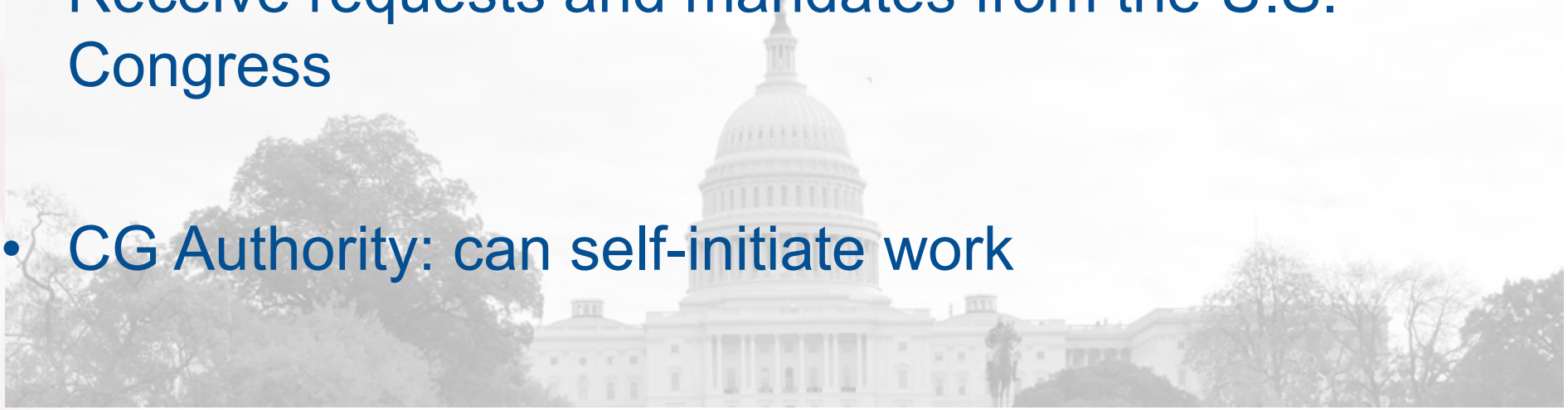
- About GAO
- Federal IT & Cybersecurity Issues
- GAO's IT Security Audits
- GAO's Challenges in Reviewing IT Security
- GAO Reports on IT Security from 2015-2016

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****.*

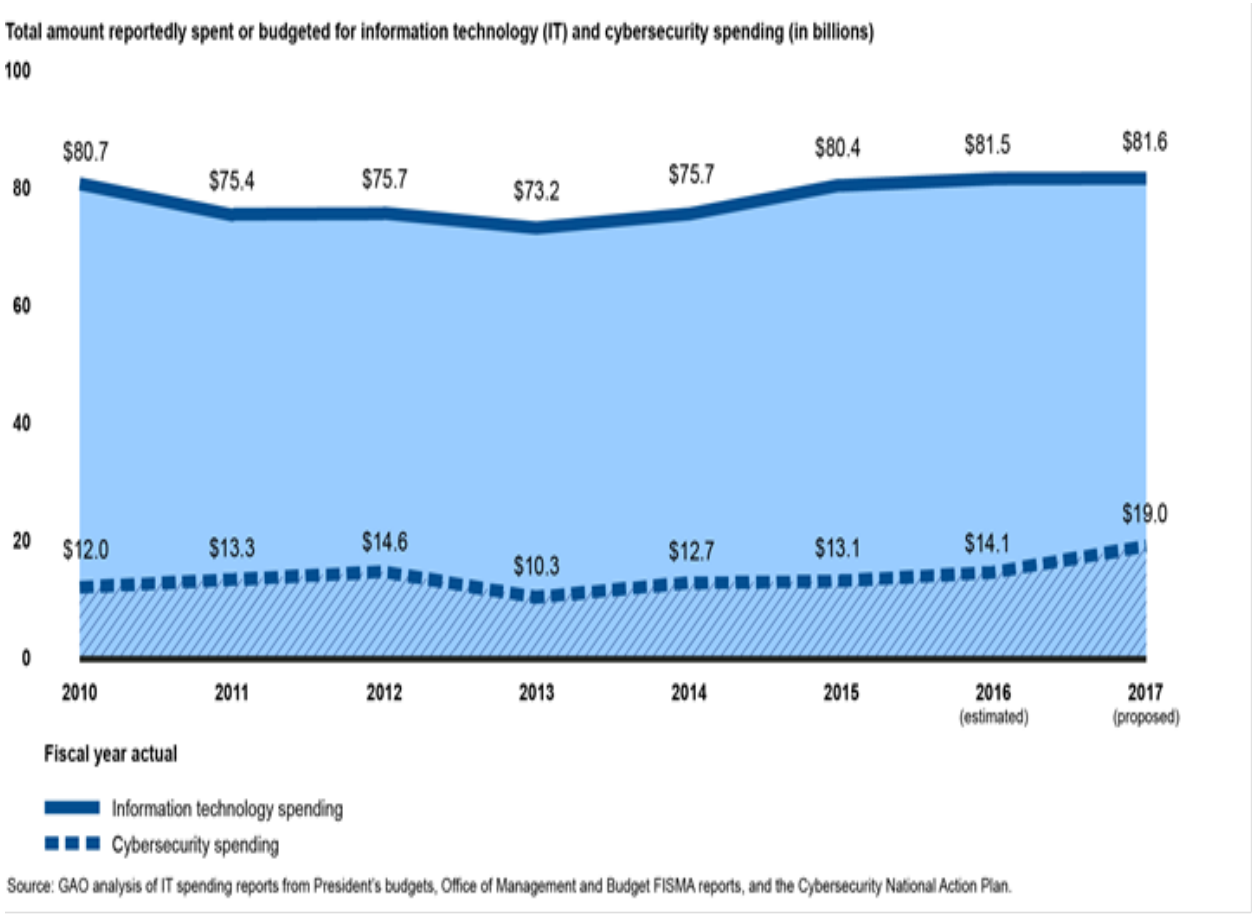
About GAO: Our Work

- 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



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.
- Proposed IT security spending for FY 17 was proposed to increase about 35 percent.



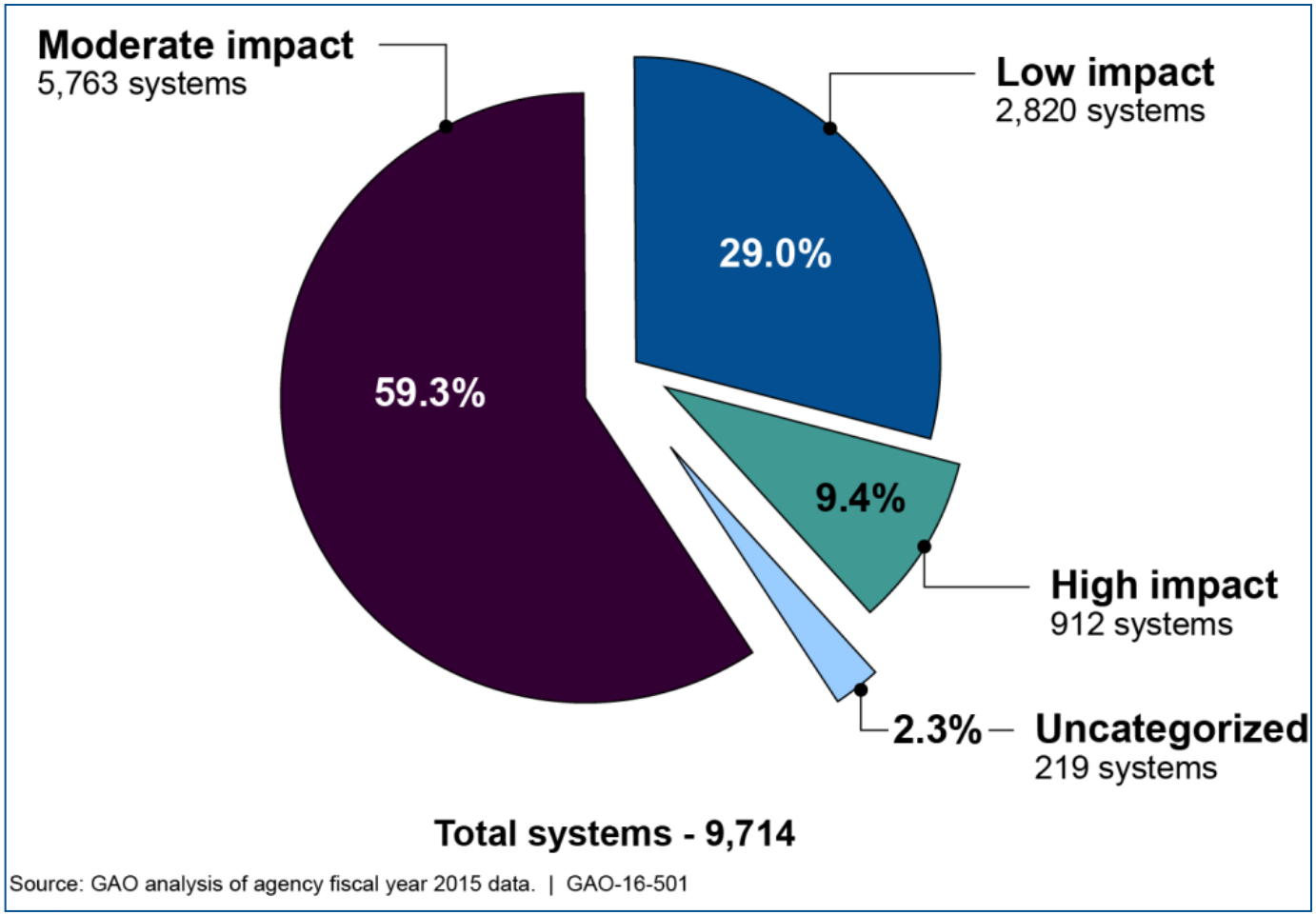
Source: GAO analysis of IT spending reports from President's budgets, Office of Management and Budget FISMA reports, and the Cybersecurity National Action Plan.

Impact of System Compromise Can be Significant

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

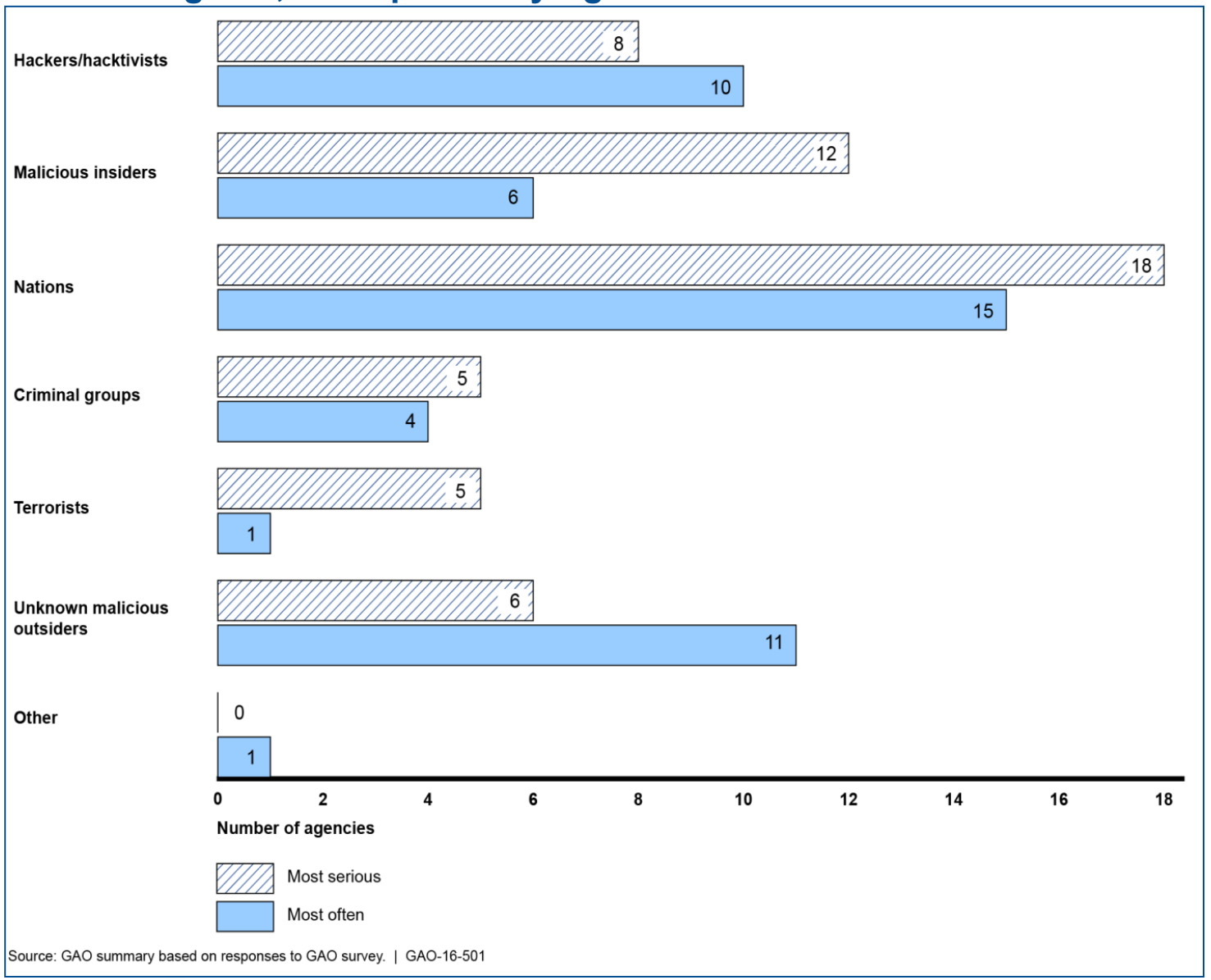


Source: GAO analysis of agency fiscal year 2015 data. | GAO-16-501

Cyber Adversaries Targeting Federal Systems

- 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

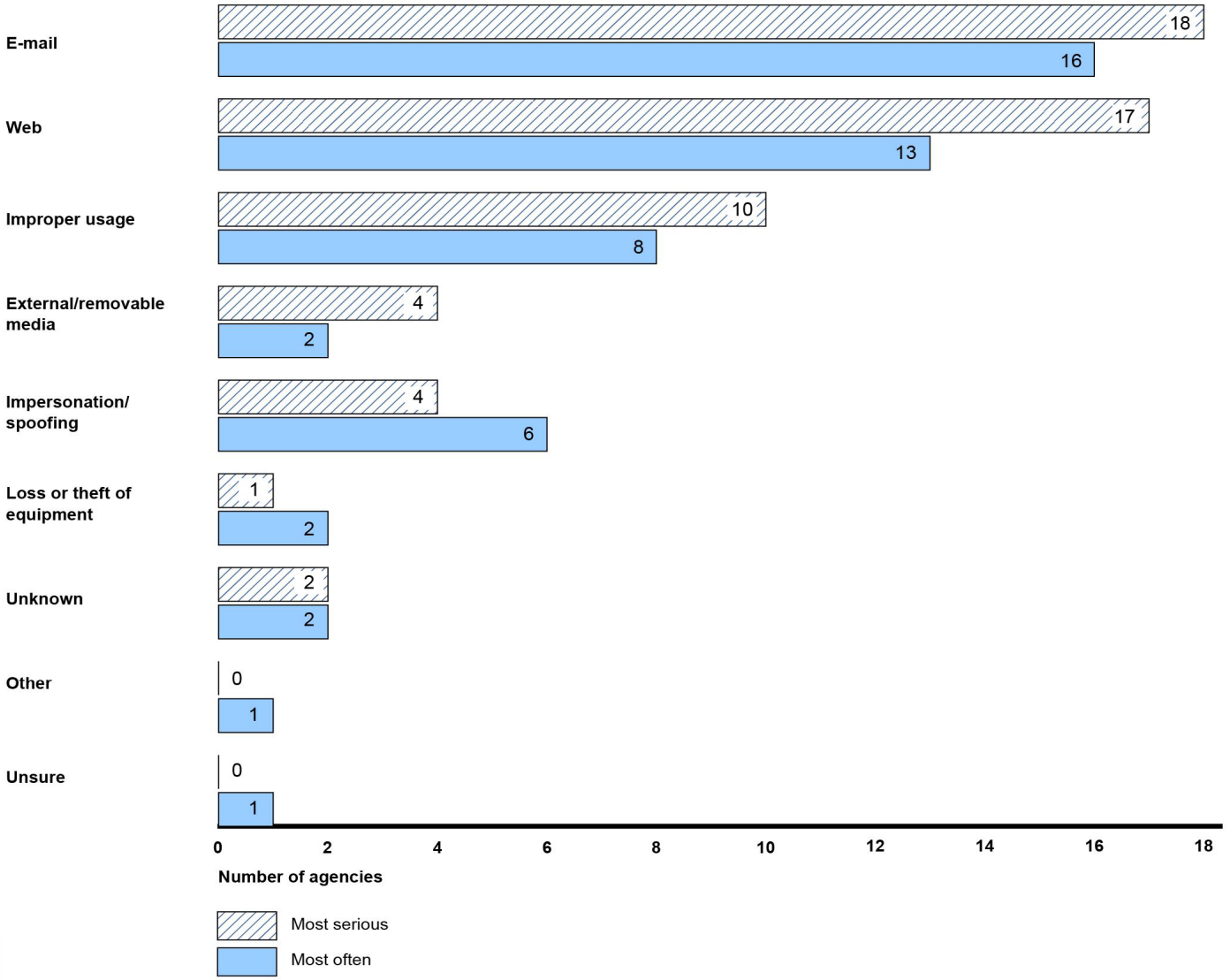


Source: GAO summary based on responses to GAO survey. | GAO-16-501

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

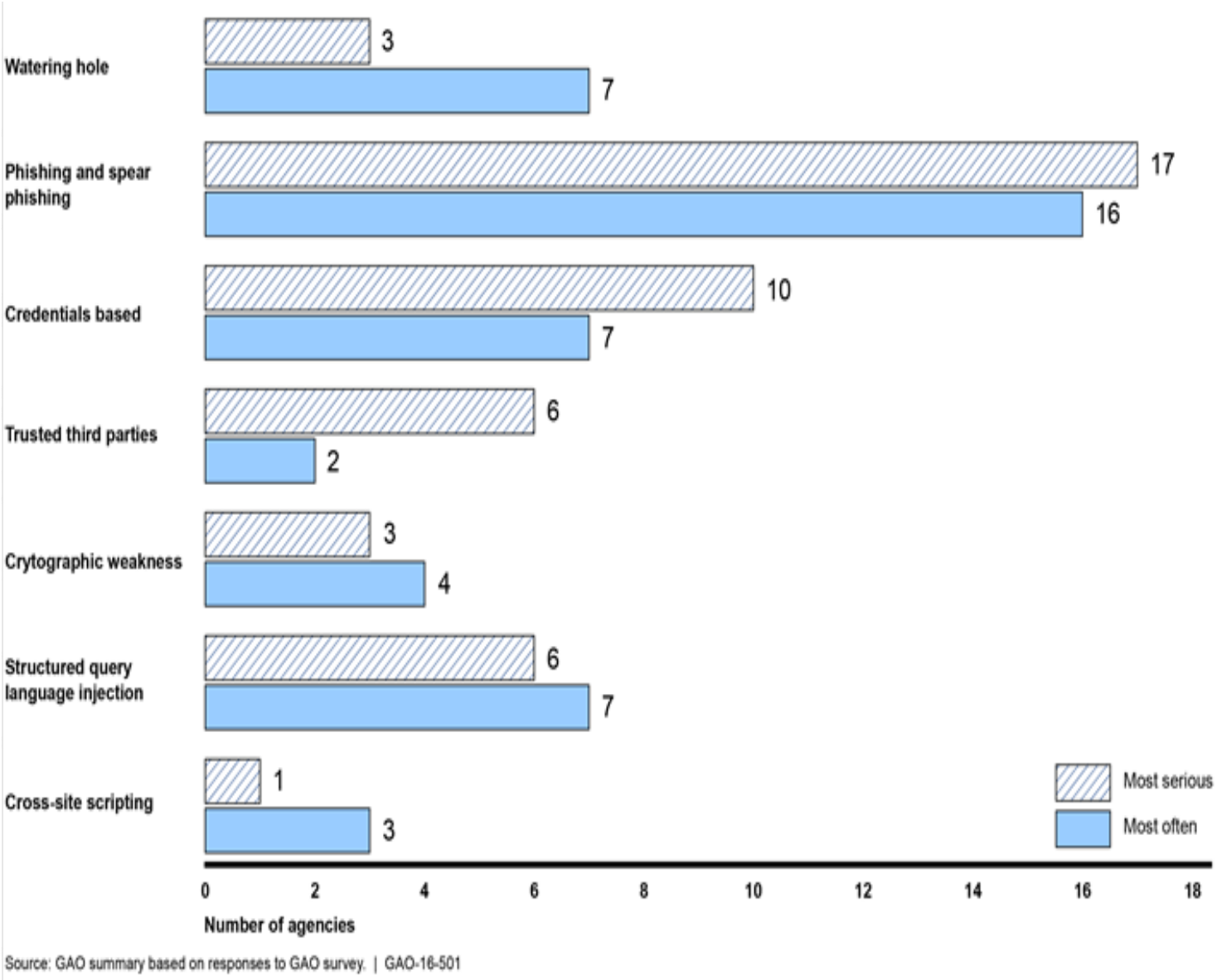


Source: GAO summary based on responses to GAO survey. | GAO-16-501

Techniques Used to Attack IT Systems

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

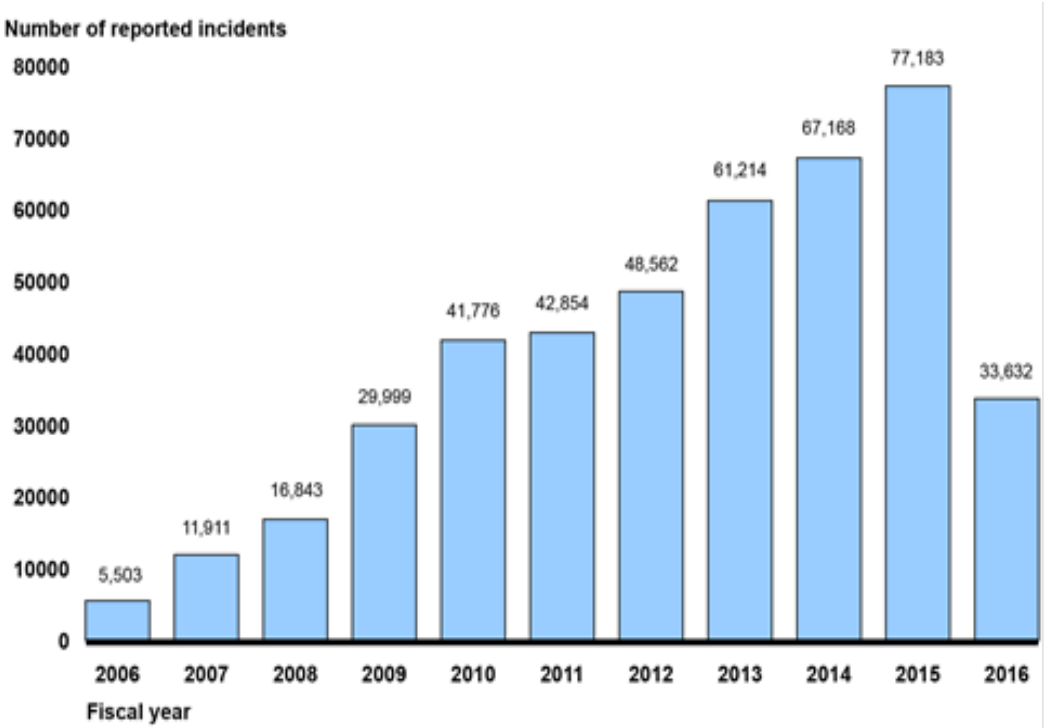
Most Serious and Most Frequently Identified Attack Techniques, as Reported by Agencies



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

Reported Security Incidents Have Risen

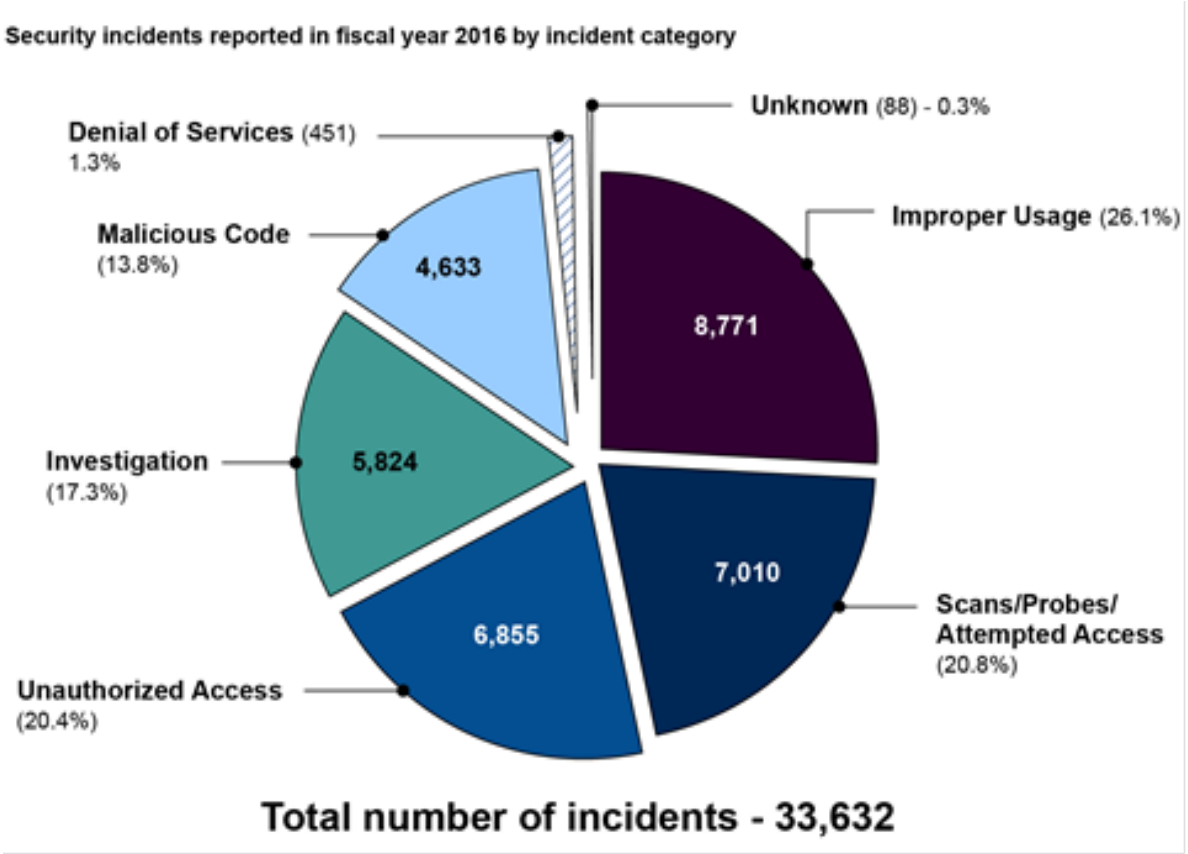
- From fiscal year 2006 through 2015, reported security incidents increased about 1,300 percent.
- Increases likely due to:
  - Better reporting
  - Better detection
  - Active threats
  - Vulnerable systems
- Steep drop in incidents reported in fiscal year 2016 likely due to changes in reporting requirements.



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

Types of Information Security Incidents

- Security incidents perpetrated by both external and internal parties.
- About 20 percent involved personally identifiable information in fiscal year 2016.



GAO

GAO's Work on IT Security:

- 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.

GAO's Work on IT Security: 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

Source of images: Microsoft Office Clip Art

GAO's Work on IT Security: Teams Involved

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

Source of images: GAO

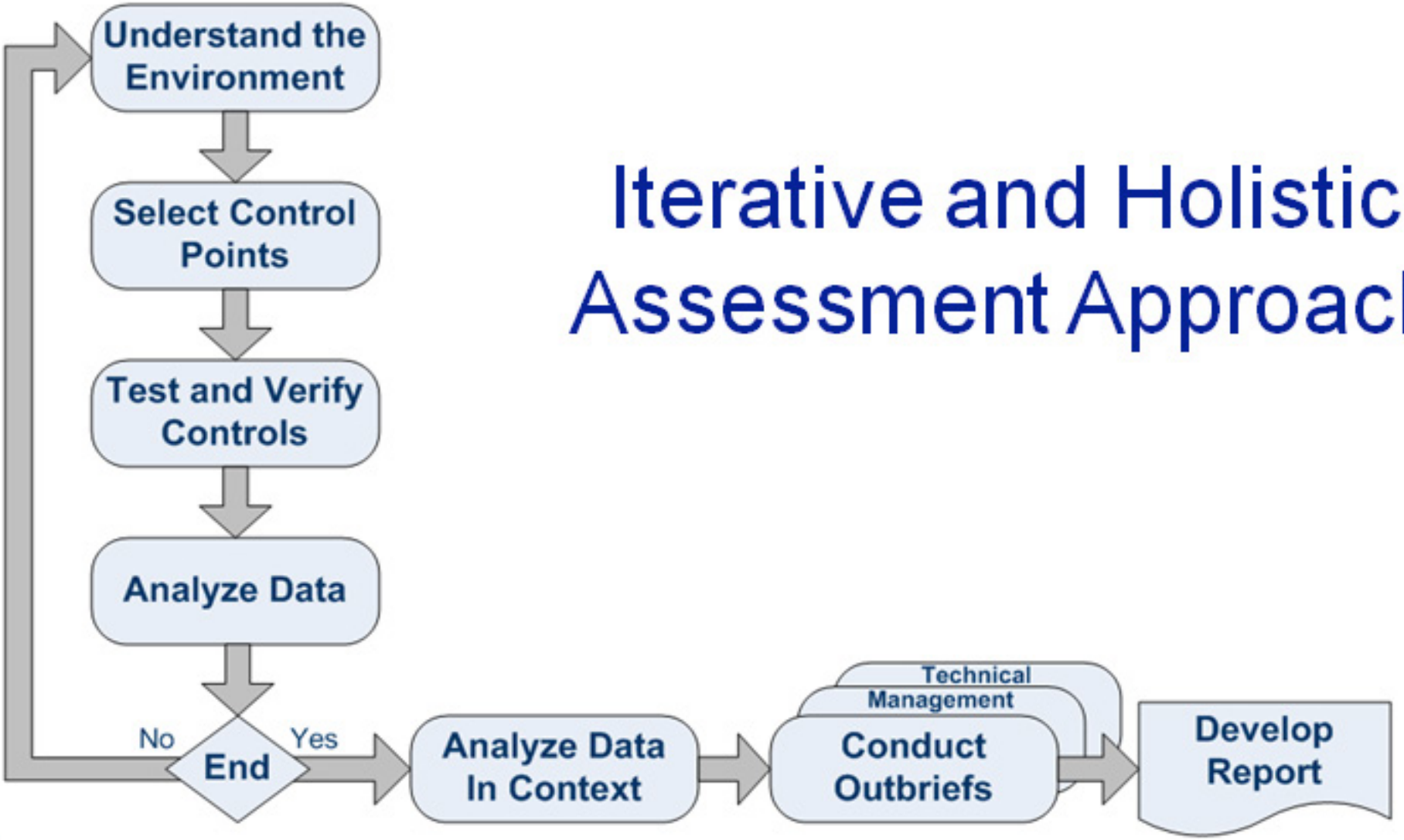
Audit methodology for assessing information security controls

- *Federal Information System Controls Audit Manual* (GAO-09-232G)
- Objective: To assess effectiveness of agency's security controls in protecting the confidentiality, integrity, and availability of its information systems and information.
- Control Categories:
  - Access controls -- Physical and Logical
  - Configuration management
  - Segregation of duties
  - Contingency planning
  - Security management

Criteria for IT Security Audits

- *Federal Information Security Modernization Act of 2014*
- *Cybersecurity Act of 2015*
- OMB Memoranda
- NIST Federal Information Processing Standards and SP 800-series
- US Government Configuration Baselines
- DISA *Security Technical Implementation Guides* (STIGs)
- Vendor Security Guidelines
- GAO's *Standards for Internal Control in the Federal Government*

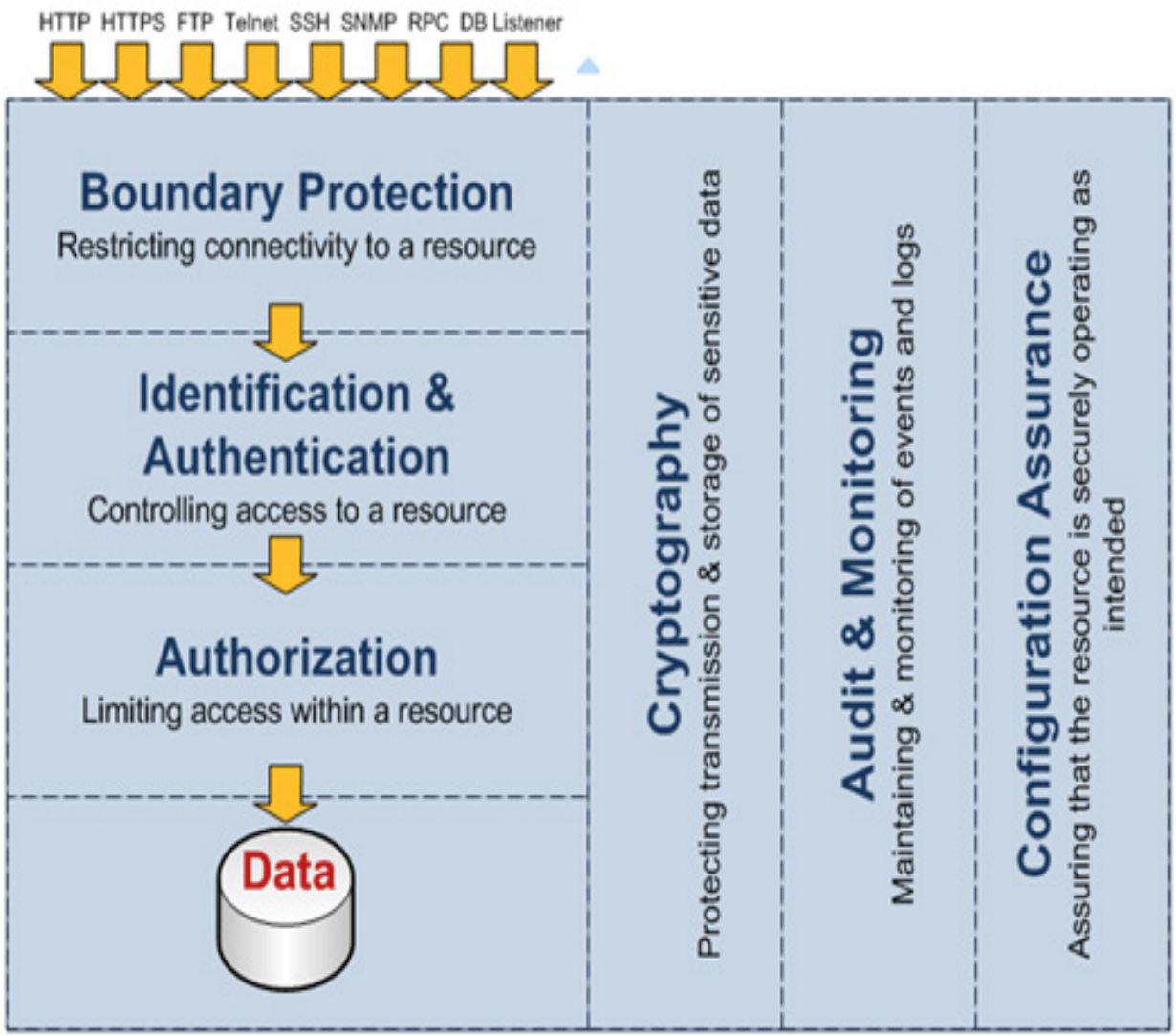
Overall audit process



Iterative and Holistic Assessment Approach

Testing logical access controls

Common Access Methods

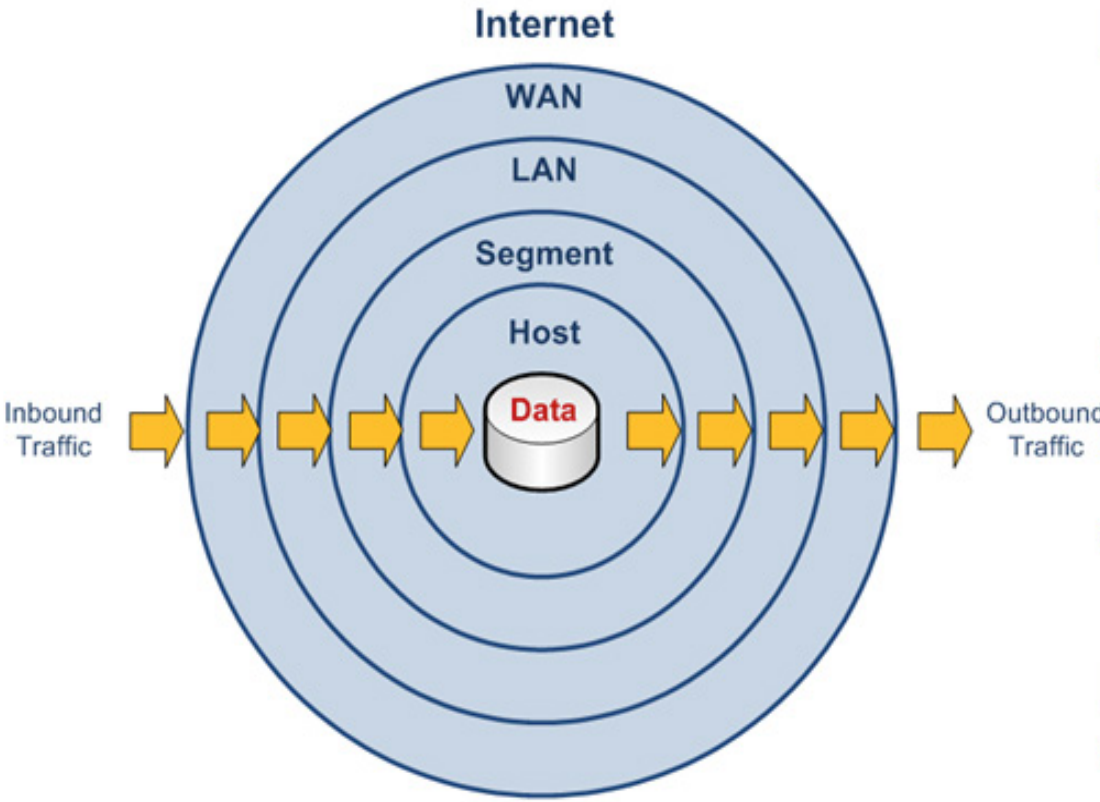


Focus on main controls that might stop an intruder, based on knowledge of latest vulnerabilities such as:

browser – Java, ActiveX, Flash, PDF

"spoofed" emails

Testing network access controls



If exploited, how does information go out? HTTP, HTTPS, DNS

Authentication of network routing protocols (EIGRP, BGP)

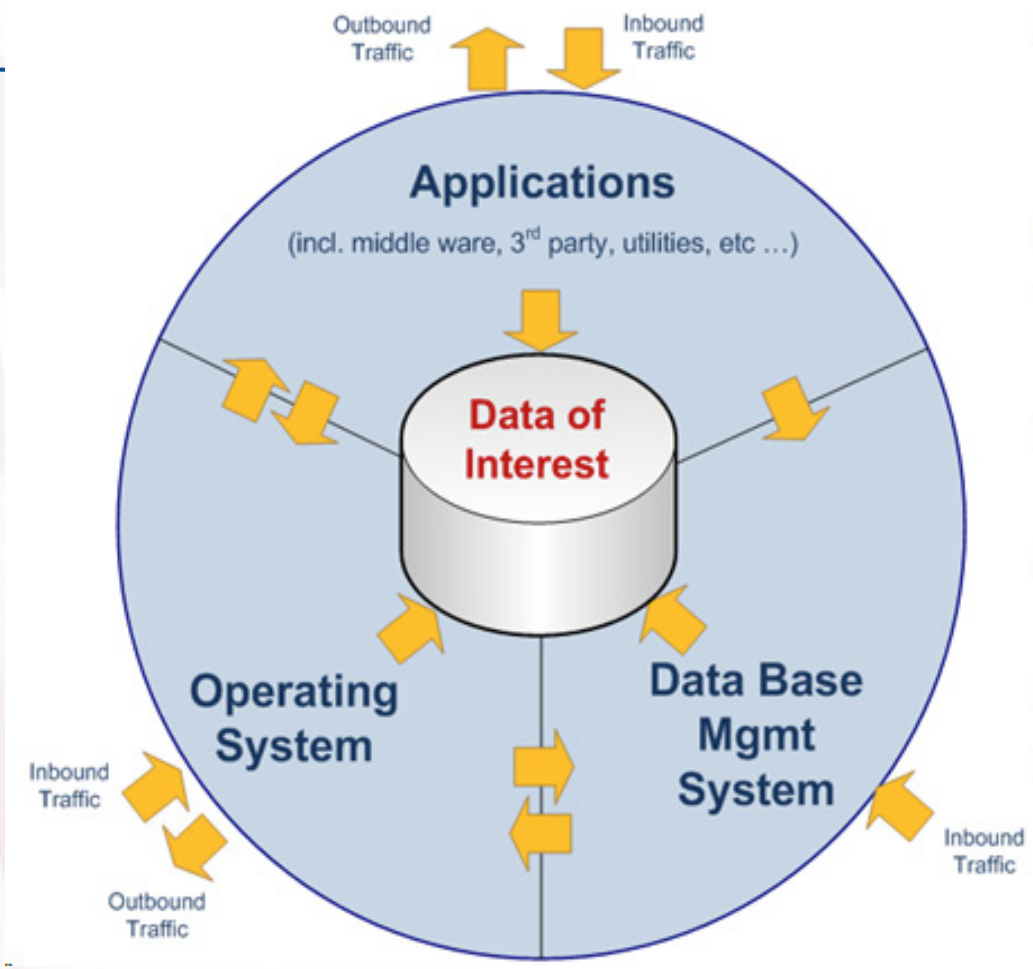
Cisco SAFE (Security Reference Architecture)

VPN – use of TLS v SSL

Firewall rules (Cisco ASA, Checkpoint, etc.)

Data loss prevention solutions

Testing host access controls



- Ask agencies to run scripts to get key configuration settings (Windows, Linux/Unix, etc)
- Database scanner
- Email server (sendmail, postfix) settings
- Internet Explorer, MS Office settings
- Conformance to vendor guidance (Microsoft, Apple)
- Up to date patches
- Virtualization – hypervisor security settings, Storage Area Network (SAN) configurations

Assess significance of findings

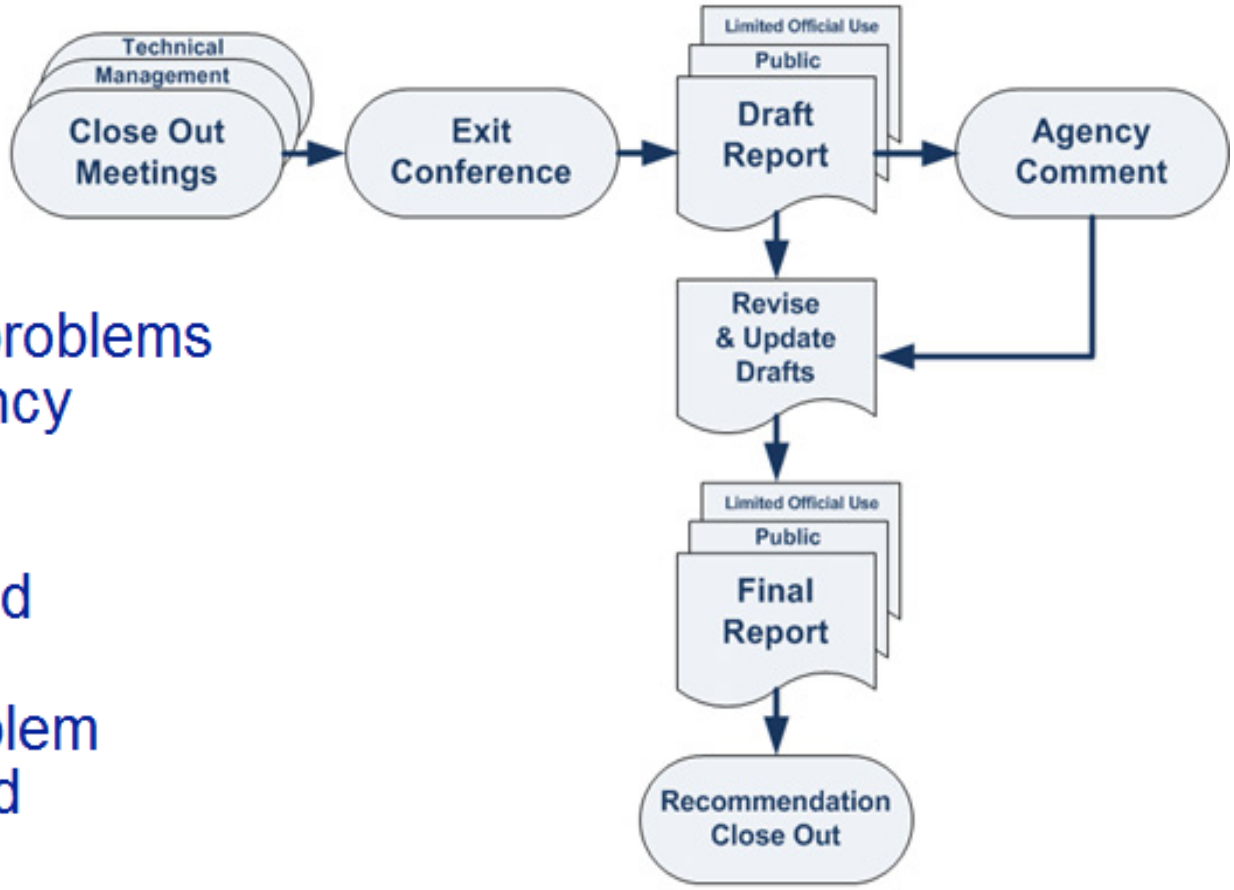
Assess vulnerabilities in the context of the network connectivity and the impact on the organization's mission.

GAO

Examine 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

Communicating results of audit



Focus on most important problems – the ones that'll help agency become more secure

Criteria – NIST, vendor and industry guidance
Condition – describe problem
Effect – explain what could happen if exploited
Cause – sometimes unclear, often related to immature information security program

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

GAO

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

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

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

Case Study: 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 Study: Air Traffic Control Systems Security

Background

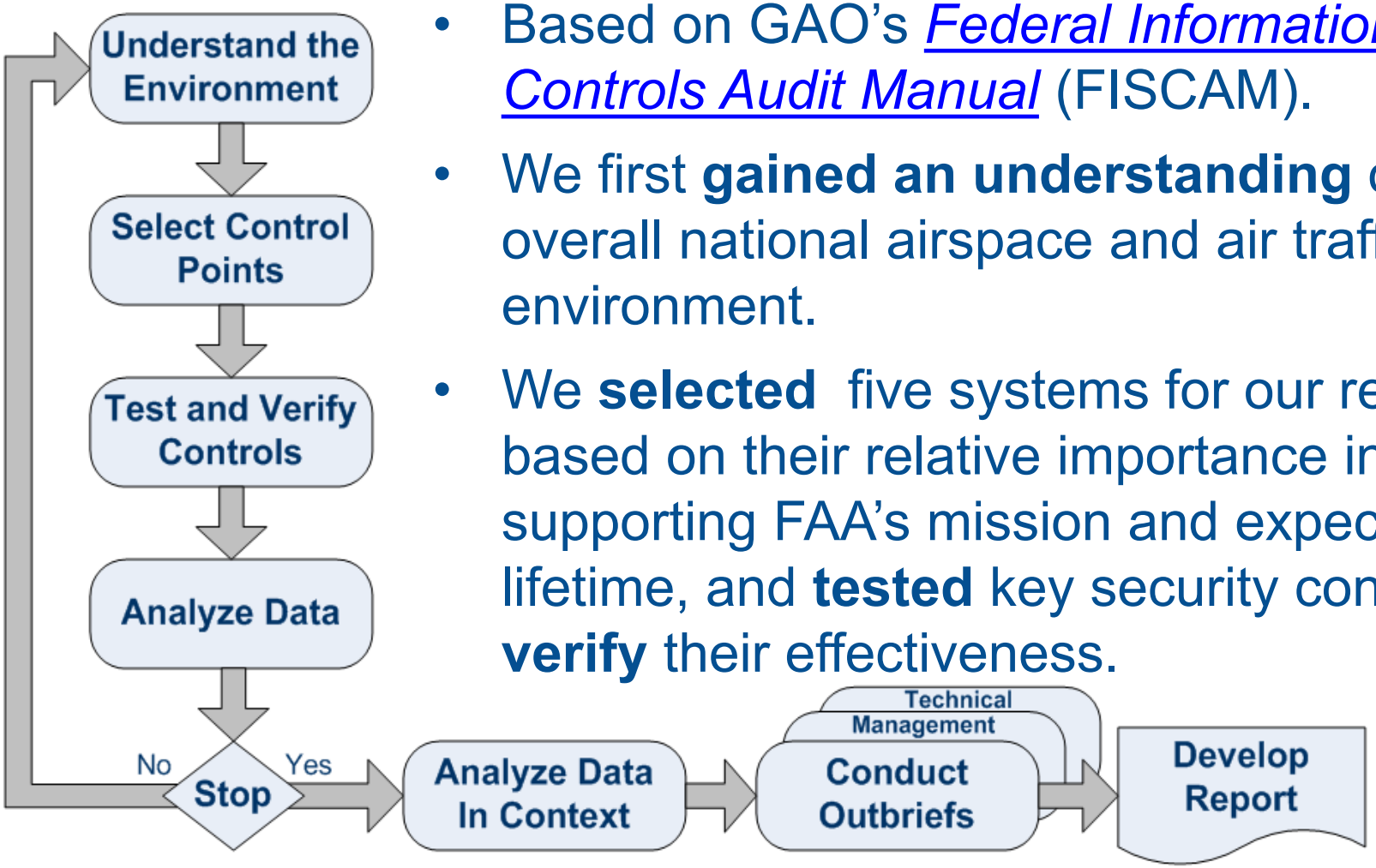
- New networking technologies connecting FAA's systems expose them to new cybersecurity risks, which increase opportunities for systems to be compromised or damaged.

Summary of Air Traffic Control over the U.S.

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

Case Study: 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 Study: 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 Study: 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.

Results of GAO Audits

- Identified information security as governmentwide high-risk area
- 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.