GAO Information Security Update

Federal Computer Security Managers' Forum
Gaithersburg, MD

Nick Marinos
Assistant Director, Information Technology

Tom Johnson
Senior IT Analyst, Information Security Issues

August 16th, 2016

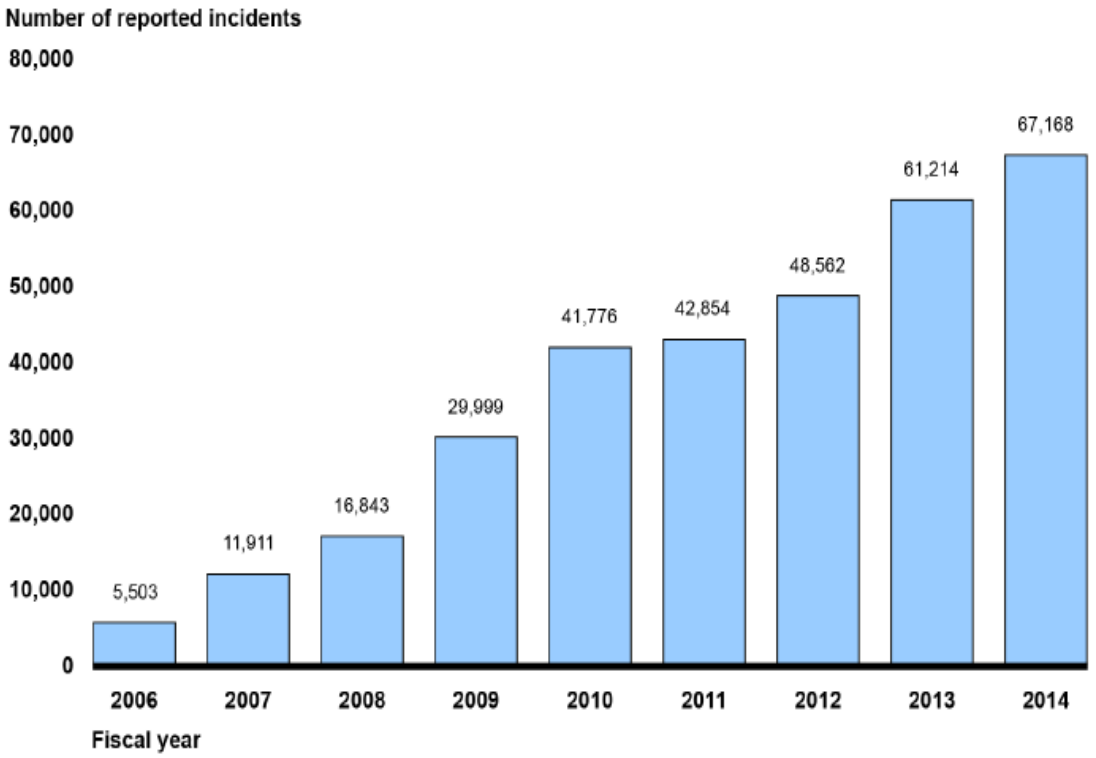
I. Federal landscape: Cyber threats

- Risks to cyber-based assets can originate from unintentional or intentional threats.
  - Unintentional threats: natural disasters, defective computer or network equipment, and careless or poorly trained employees
  - Intentional threats: both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists.
- Adversaries vary in terms of their capabilities, willingness to act, and motives, which can include seeking monetary gain or a political, economic, or military advantage.

Federal Cybersecurity and Privacy: Why High Risk?

- Since FY2006, the number of information security incidents affecting systems supporting the federal government has steadily increased each year.
- The number of reported security incidents involving PII at federal agencies has more than doubled in recent years—from 10,481 incidents in FY2009 to 27,624 incidents in FY2014.

Figure 1: Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2014



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014. | GAO-15-758T

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

Evaluating Cybersecurity: Recent GAO Reviews

- Performance Audits
  - High Impact Systems
    - GAO-16-501
  - Healthcare.gov
    - GAO-16-265
  - National Cybersecurity Protection System
    - GAO-16-294
  - Cybersecurity Framework
    - GAO-16-152
  - Critical Infrastructure Protection
    - GAO-16-79
  - Vehicle Cybersecurity
    - GAO-16-350
- Annual Financial Statement Audit Support
  - Internal Revenue Service (IRS)
    - GAO-16-398
  - Federal Deposit Insurance Corporation (FDIC)
    - GAO-16-605
  - Securities and Exchange Commission (SEC)
    - GAO-16-493

Emerging Trends in GAO Work

- Increased emphasis on Public-Private partnerships and assessing how the Federal Government helps to improve the security of the public sector. Also extends to Federal-State relationships through initiatives like healthcare.gov and the state healthcare exchanges.
- Additional focus, due to high profile breaches, on sensitive data that the government maintains and how it protects that data
- Assessing systems that are contracted to be maintained, hosted and developed off-site and how agencies ensure that their data is adequately protected. Including cloud based solutions and SaaS/PaaS initiatives.
- Detecting insider threats and preventing the exfiltration of sensitive data.

Developments that will impact our work

- High profile breaches
- Updated OMB Memoranda A-130
- Updated OMB Memoranda A-123
- FITARA
- FISMA 2014

The Questions That Keep Coming Up on the Audit Trail

- How are agencies measuring the effectiveness of guidance provided to the private sector?
- 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?

Resources

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