Evaluating the Cybersecurity and Privacy of Federal Information Systems

Presentation to the
Mid-America Intergovernmental Audit Forum

Overland Park, Kansas

Nick Marinos
Assistant Director, Information Technology
202-512-9342; marinosn@gao.gov

December 4, 2015

Agenda

I. Federal cybersecurity and privacy landscape: emerging risks, trends, and recent events

II. What are federal agencies doing to protect information?

III. Evaluating cybersecurity programs at federal agencies

GAO

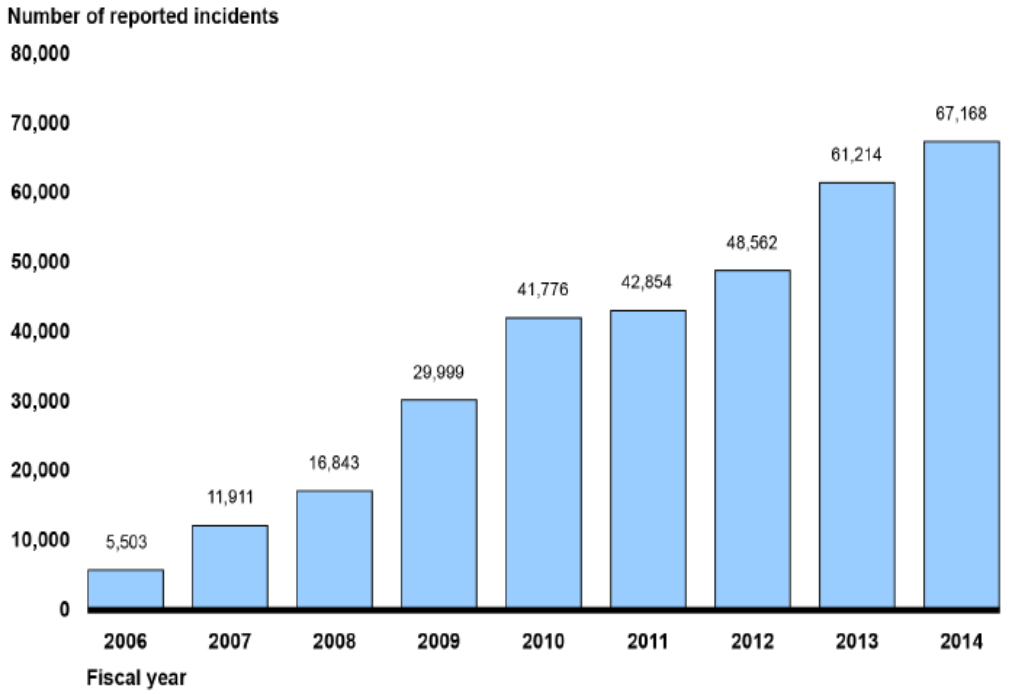
I. Federal landscape: Cyber threats

- 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.

I. Federal landscape: Trends

- 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

I. Federal landscape: Recent events

- June 2015, Office of Personnel Management (OPM): reported that an intrusion into its systems affected personnel records of about 4 million current and former federal employees. Separate incident on OPM systems related to background investigations affected 21.5 million individuals, including 5.6 million whose fingerprint data was stolen.
- June 2015, Internal Revenue Service (IRS): reported that criminals used taxpayer-specific data acquired from non-IRS sources to access information on over 300,000 tax accounts. These data included Social Security information, dates of birth, and street addresses.
- September 2014, U.S. Postal Service (USPS): reported a cyber-intrusion may have compromised PII for more than 800,000 of its employees.

II. What are Federal Agencies Doing to Protect Information?

- Personal Identity Verification (PIV)
  - Implement secure and reliable forms of identification for federal employees and contractor personnel who access government-controlled facilities and information systems.
- Continuous Diagnostics and Monitoring (CDM)
  - Provide federal departments and agencies with capabilities and tools that identify cyber risks on an ongoing basis, prioritize based on potential impacts, and enable personnel to mitigate the most significant problems first.

GAO

II. What are Federal Agencies Doing to Protect Information?

- National Cybersecurity Protection System (aka “EINSTEIN”)
  - A suite of capabilities intended to detect and prevent malicious network traffic from entering and exiting federal civilian government networks.
- 30-day Cybersecurity Sprint (June 2015)
  - Focused on deploying indicators of compromise, patching critical vulnerabilities, tightening privileged users policies and procedures, and leveraging multi-factor authentication.
  - Agencies were to report to OMB and DHS on progress and challenges within 30 days.

III. Evaluating Cybersecurity Programs: Recent GAO reviews

- Performance Audits – Agency Specific Reviews
  - FAA Air Traffic Controls Systems - GAO-15-221
  - Library of Congress – IT Management Review - GAO-15-315

- Performance Audits – Government-wide Reviews
  - Contractor Oversight of Privacy/Security Controls – GAO-14-612
  - Federal Information Security/FISMA Report - GAO-15-714

- Annual Financial Statement Audit Support
  - Internal Revenue Service (IRS) – GAO-15-337
  - Federal Deposit Insurance Corporation (FDIC) – GAO-15-426
  - Securities and Exchange Commission (SEC) – GAO-14-419

GAO

III. Evaluating Cybersecurity Programs: Cybersecurity program audit health check

- Does the agency know its IT environment?
  - Check for a comprehensive and up-to-date inventory of systems that includes the type of data processed on those systems. (NIST special publication 800-18 and FIPS-199)
- Are security and privacy risks routinely and inclusively assessed by the agency?
  - Check to ensure that mission owners are actively involved in performing security risk assessments and privacy impact assessments of information systems. (NIST special pub. 800-30)

GAO

III. Evaluating Cybersecurity Programs: Cybersecurity program audit health check

- Are tests of the effectiveness of automated security protections performed?
  - When automated tools are relied upon for testing, make sure the tools are tested too and correct any identified weaknesses. (NIST special pubs. 800-53 rev. 4 and 800-53A)
- In information on known weaknesses and vulnerabilities shared with agency leadership?
  - Make sure that the state of security, including efforts to address vulnerabilities, is communicated to leadership/decision makers. (NIST special pub. 800-100)

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