CYBERSECURITY: Update from the U.S. Government Accountability Office

Nick Marinos
Director, Cybersecurity & Information Management Issues
Information Technology Team
U.S. Government Accountability Office
May 15, 2018
Agenda

• About GAO’s Information Technology Team
• Risk-based Approaches to Evaluate the Effectiveness of Cybersecurity Processes and Controls
• Recent GAO Cybersecurity Reports/Products
• Emerging Issues
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

Establishing a national cybersecurity strategy and effective government-wide action and oversight

• Evaluate efforts to develop and implement a national cybersecurity strategy
• Assess federal efforts to address global cyber challenges, including cyber defense and response efforts
• Examine the implementation of government-wide cybersecurity initiatives

Ensuring the effectiveness of agency programs for the protection of federal information and systems

• Report to Congress on the effectiveness of federal agency cybersecurity
• Assess the effectiveness of security programs, policies, practices, and controls
• Evaluate the cybersecurity of major systems development and acquisition
• Assess agency preparedness for, and response to, breaches of sensitive government information

Strengthening the federal role in the public-private partnership for the protection of critical infrastructure and sensitive data

• Study cybersecurity implication of emergency technologies (IoT, Artificial Intelligence)
• Evaluate federal oversight of programs supporting the nation’s critical infrastructure
• Examine federal efforts to oversee safeguarding of personal and other sensitive data shared with private-sector and other non-federal entities
• Examine federal response to security incidents with national ramifications, such as cyberattacks and data breaches at critical infrastructure components
How GAO Scopes Cybersecurity and Privacy Audits

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

• 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.)
Recent Reports

CRITICAL INFRASTRUCTURE PROTECTION

Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption

Recent Reports

http://www.gao.gov/products/GAO-17-549
Emerging Issues

- Cybersecurity Workforce Challenges
- Public-Private Sharing of Cyber Threat Information
- Impact of Equifax Breach on Consumers and the Federal Government
- Effectiveness of Cybersecurity Risk Management Programs
- Impact of Federal Cybersecurity Requirements on States
- Cybersecurity Posture of Specific Critical Infrastructure Sectors (Electricity Grid, Oil & Gas Pipeline Subsector)