Office of Management and Budget: Privacy Policy and Oversight

Charlie Cutshall
Privacy Branch | OIRA | OMB
Disclaimer

• This presentation provides a general overview of some of the requirements in the Paperwork Reduction Act, Privacy Act, and E-Government Act.

• This presentation does not:
  o Provide legal advice or interpretations.
  o Offer interpretations of OMB policies.
  o Establish or modify any OMB policies.

• Nothing in this presentation may be used or cited for any official purpose.
Overview

• Intro to Privacy in the Federal Government
• The Fair Information Practice Principles
• The Role of OMB: Privacy Policy & Oversight
• OMB Circular A-130
• Annual FISMA Report to Congress
• FISMA SAOP Metrics
June 25, 1973
Fair Information Practice Principles

1. Access and Amendment
2. Accountability
3. Authority
4. Minimization
5. Quality and Integrity
6. Individual Participation
7. Purpose Specification and Use Limitation
8. Security
9. Transparency
The Privacy Act

(v) Office of Management and Budget

Responsibilities.—The Director of the Office of Management and Budget shall—

(1) develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for the use of agencies in implementing the provisions of this section; and

(2) provide continuing assistance to and oversight of the implementation of this section by agencies.
Sec. 3504. Authority and functions of Director

(g) With respect to privacy and security, the Director shall--

(1) develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies;

(2) oversee and coordinate compliance with sections 552 and 552a of title 5, the Computer Security Act of 1987 (40 U.S.C. 759 note), and related information management laws.
The Office of Information and Regulatory Affairs (OIRA)

- Established by the Paperwork Reduction Act
- Administrator appointed by the President and Senate confirmed.
- The Director shall delegate to the Administrator the authority to administer all functions under this chapter ...
- **The Administrator shall serve as principal adviser to the Director on Federal information resources management policy.**
OMB Circular A-130

• Provides general policy for the planning, budgeting, governance, acquisition, and management of Federal Information as a strategic resource

• Pertains to information resources, which can include information, information systems, technology, equipment, infrastructure, personnel, funds, etc.
• Elevates the role and status of the SAOP to be a coequal partner with agency counterparts.
• Helps agencies transition from privacy as merely a compliance exercise to privacy as a strategic, comprehensive, continuous, risk-based program.
• Requires better coordination between privacy and security officials.
Annual FISMA Report


• Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the **effectiveness of information security policies and practices** during the preceding year.

FISMA SAOP Metrics

• SAOP FISMA Metrics:
  
  • CyberScope (**Quantitative Metrics**)
    Agencies report on compliance with various privacy requirements principally sourced from Circular A-130. Metrics include 84 questions divided into 14 categories.
  
  • Annual FISMA Guidance (**Qualitative Metrics**)
    Agencies provide privacy program plans and policies, including Breach Response plan, Privacy Continuous Monitoring strategy, Privacy Program plan, SSN reduction policy.
FY 2018 FISMA SAOP Metrics

Contents
Document History ................................................................................................................. 2
1. General Privacy Program Requirements ................................................................. 4
2. Information Systems ............................................................................................... 4
3. Information Technology Systems and Privacy Impact Assessments ....................... 5
4. Systems of Records ................................................................................................. 6
5. Considerations for Managing PII ........................................................................... 7
6. Social Security Numbers ......................................................................................... 8
7. Digital Services ....................................................................................................... 8
8. Budget and Acquisition .......................................................................................... 9
9. Contractors and Third Parties ............................................................................... 10
10. Workforce Management ...................................................................................... 11
11. Training and Accountability .................................................................................. 11
12. Incident Response ................................................................................................. 12
13. Risk Management Framework ............................................................................. 13
14. Privacy Program Website ...................................................................................... 14

Available: www.DHS.gov/FISMA
Review

• Intro to Privacy in the Federal Government
• The Fair Information Practice Principles
• The Role of OMB: Privacy Policy & Oversight
• OMB Circular A-130
• Annual FISMA Report to Congress
• FISMA SAOP Metrics
Contact Information

Charlie Cutshall
CCutshall@omb.eop.gov