Privacy and Security Challenges in the Information Age

June 6, 2008

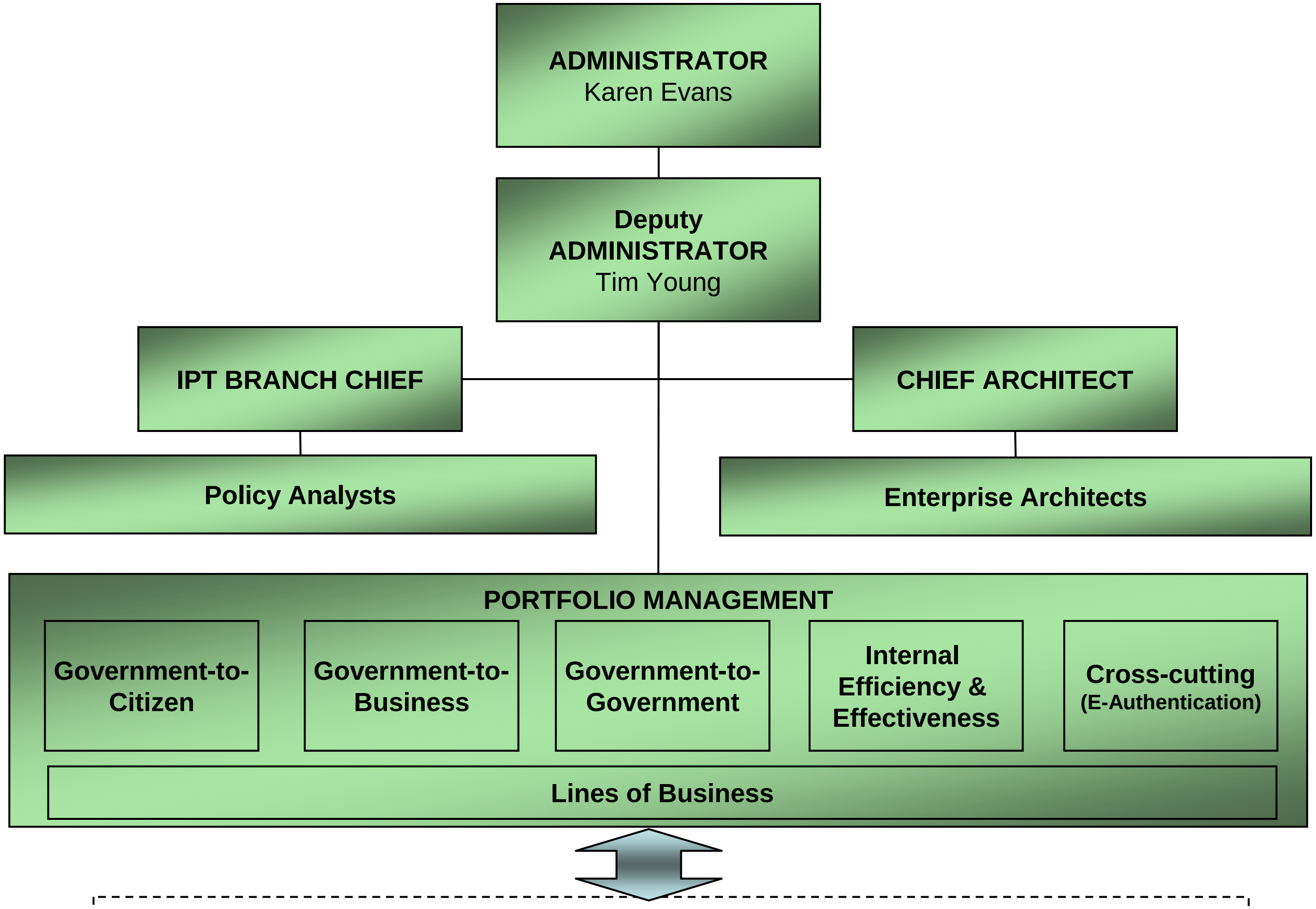
John Lee
E-Government and IT
Office of Management and Budget

E·GOV

Agenda

- Background/Overview
- Legislation
- Security
- Privacy
- Q&A

OMB / E-Gov Organization



ADMINISTRATOR
Karen Evans

Deputy ADMINISTRATOR
Tim Young

IPT BRANCH CHIEF

CHIEF ARCHITECT

Policy Analysts

Enterprise Architects

PORTFOLIO MANAGEMENT

Government-to-Citizen

Government-to-Business

Government-to-Government

Internal Efficiency & Effectiveness

Cross-cutting
(E-Authentication)

Lines of Business

Cross-Agency Councils
Chief Information Officers (CIO)
Chief Financial Officers (CFO)
Chief Acquisition Officers (CAO)
Chief Human Capital Officers (CHCO)

President's Management Agenda

Overall goals of the President's Management Agenda (PMA)

- Citizen-centered
- Results-oriented
- Market-based

PMA Agenda for the Federal Government

- Improve management and performance
- Focus on deficiencies that can deliver measurable concrete results
- Include five Government-wide initiatives and 10 program-specific initiatives

"Our success depends on agencies working as a team across traditional boundaries to better serve the American people, focusing on citizens rather than individual agency needs…" - ***President George W. Bush***

Five PMA Government-Wide Initiatives

1. **Strategic Management of Human Capital**

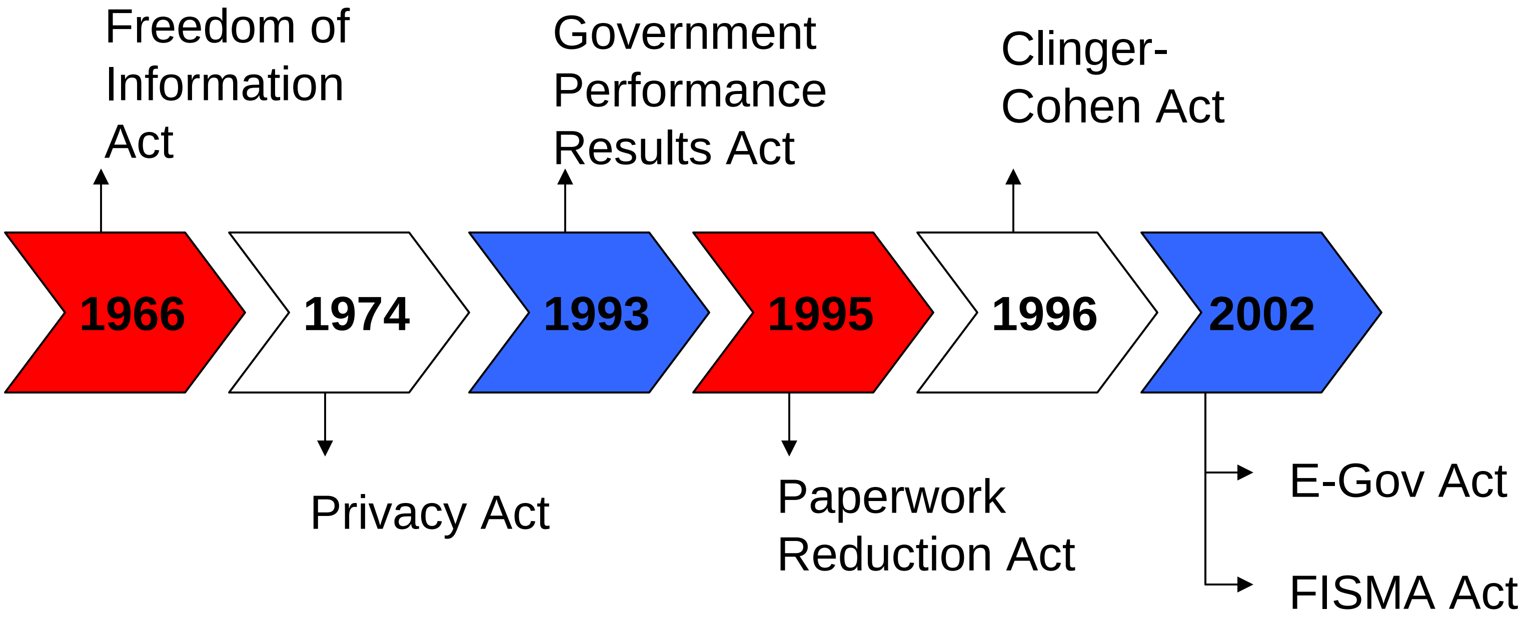
2. **Competitive Sourcing**

3. **Improved Financial Performance**

4. **Expanded Electronic Government** - Ensuring the Federal Government's $71 billion annual investment in information technology (IT) significantly improves the government's ability to serve citizens, and that IT systems are secure, and delivered on time and on budget; and

5. **Budget and Performance Integration**

Legislative Background of E-Gov



1966 – Freedom of Information Act

1974 – Privacy Act

1993 – Government Performance Results Act

1995 – Paperwork Reduction Act

1996 – Clinger-Cohen Act

2002 – E-Gov Act

2002 – FISMA Act

FISMA Act of 2002

Goal: Develop a comprehensive framework to protect the government's information, operations, and assets.

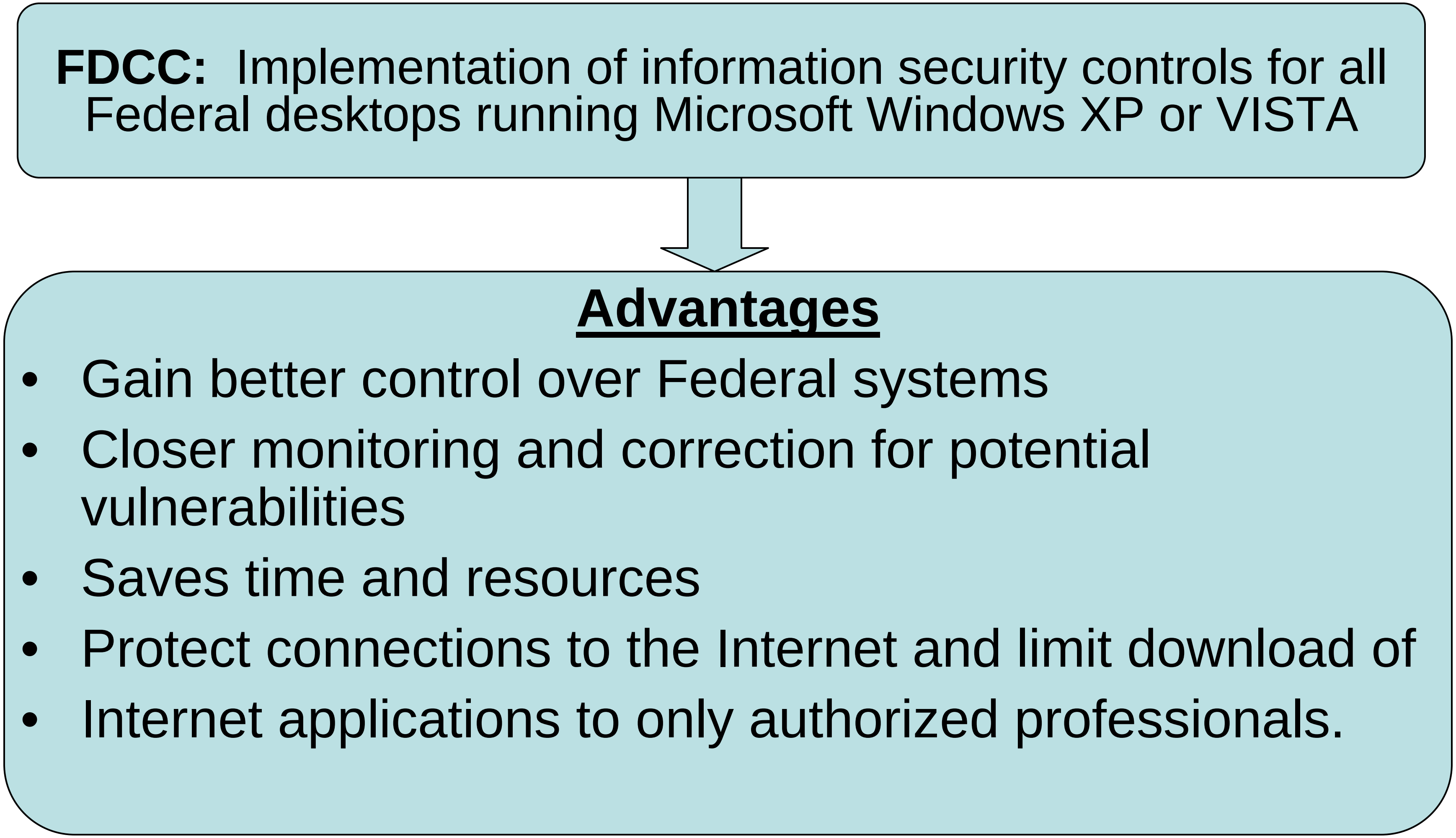
Responsibilities: FISMA assigns specific responsibilities to Federal agencies, NIST and OMB to strengthen IT system security.

FISMA Reporting Requirements

Agency Annual FISMA Report to OMB includes the following:

- Transmittal Letter from Agency Head
- Section B (CIO)
- Section C (IG)
- Section D (SAOP)
- Privacy Attachments (4)

Federal Desktop Core Configuration (FDCC)

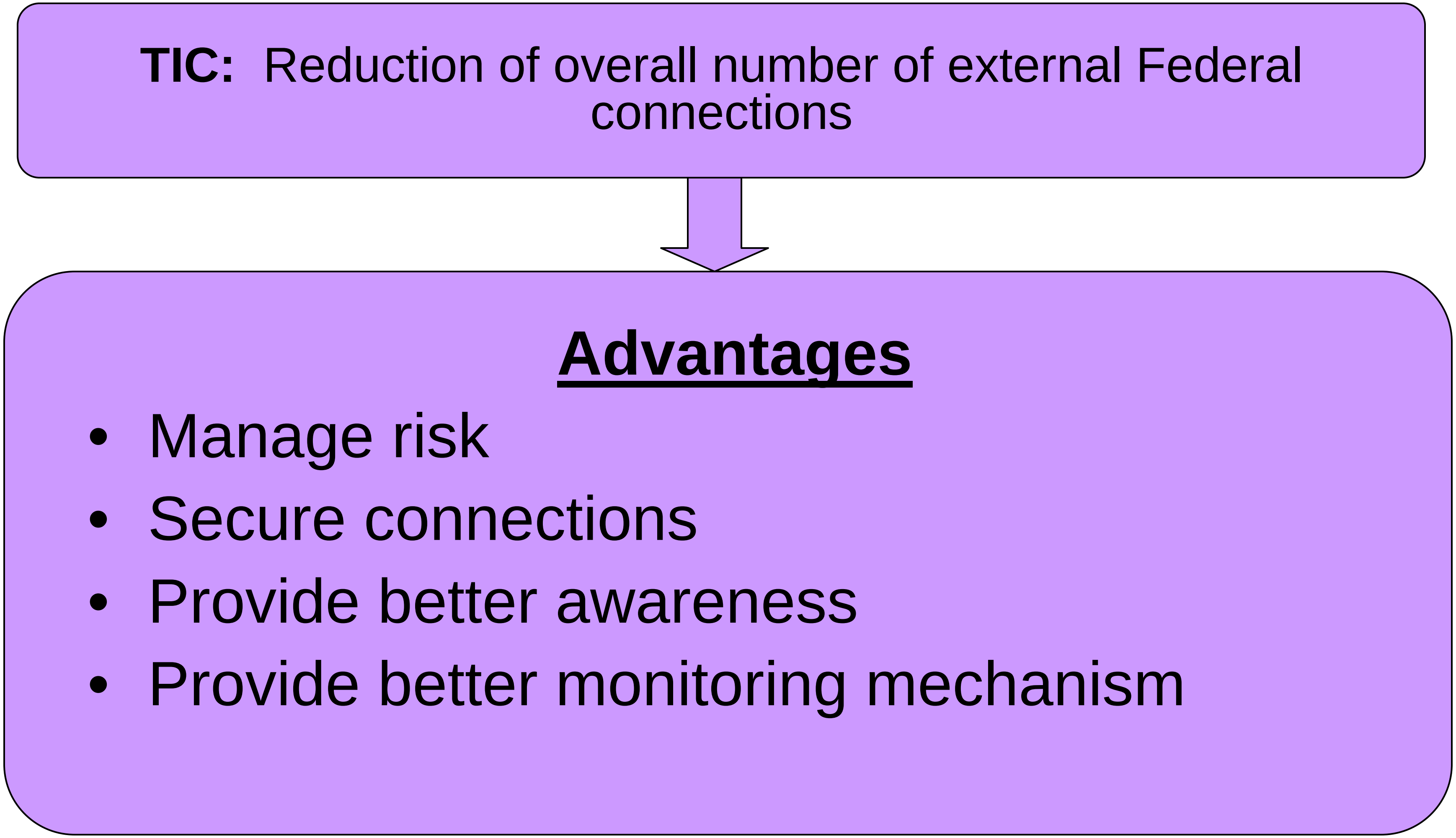


FDCC: Implementation of information security controls for all Federal desktops running Microsoft Windows XP or VISTA

Advantages

- Gain better control over Federal systems
- Closer monitoring and correction for potential vulnerabilities
- Saves time and resources
- Protect connections to the Internet and limit download of
- Internet applications to only authorized professionals.

Trusted Internet Connections (TIC)

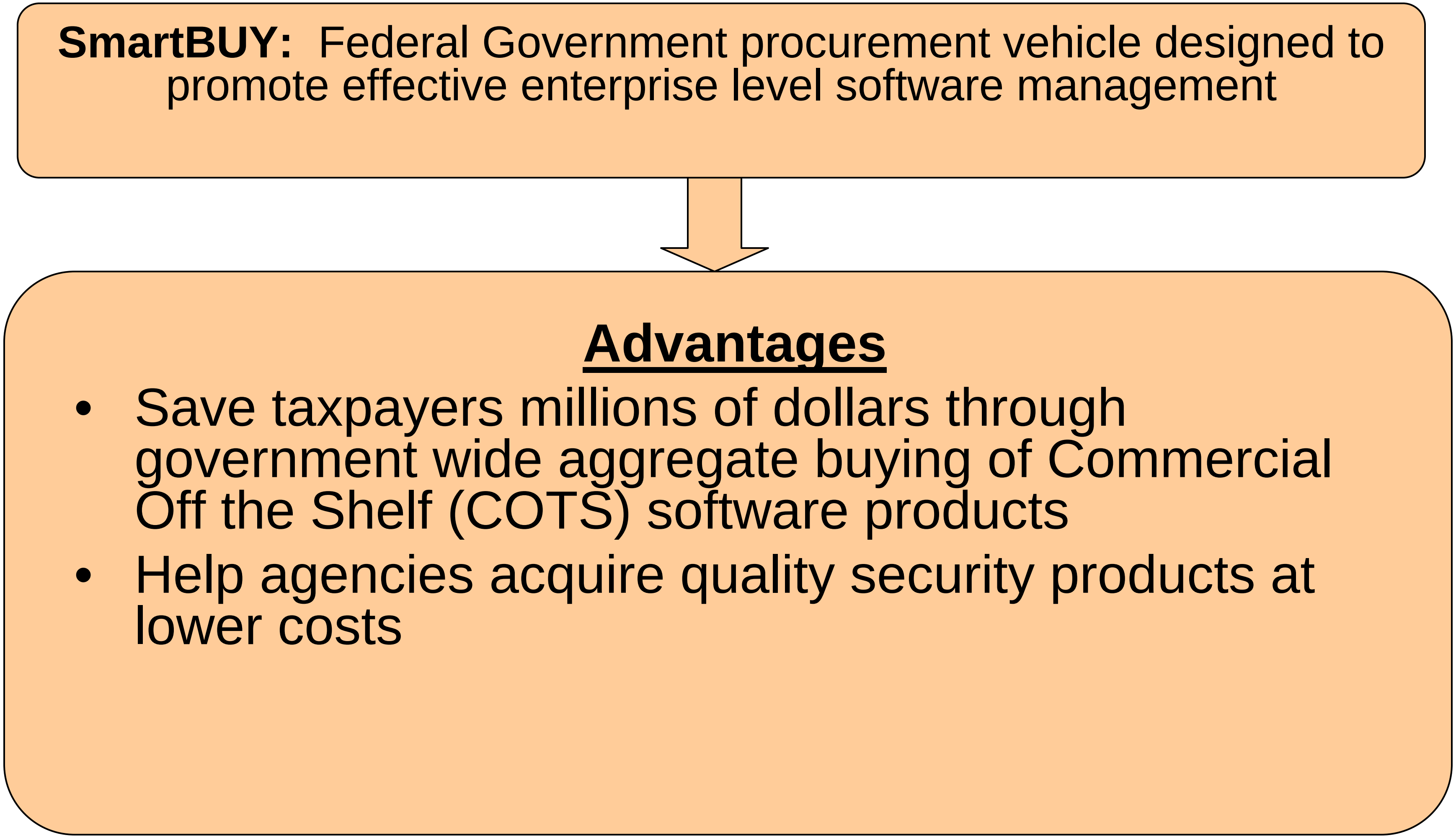


TIC: Reduction of overall number of external Federal connections

Advantages

- Manage risk
- Secure connections
- Provide better awareness
- Provide better monitoring mechanism

SmartBUY



SmartBUY: Federal Government procurement vehicle designed to promote effective enterprise level software management

Advantages

- Save taxpayers millions of dollars through government wide aggregate buying of Commercial Off the Shelf (COTS) software products
- Help agencies acquire quality security products at lower costs

Privacy Act of 1974

"The purpose of the Privacy Act is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy…"

Policy Objectives:

(1) To restrict disclosure of personally identifiable information maintained by federal agencies

(2) To grant individuals access to federal agency records maintained on individuals

(3) To grant individuals the right to amend federal agency records

(4) To establish a code of "fair information practices," to comply with statutory norms

Protection against Identity Theft

1. **Creation of Federal Identity Theft Task Force (Executive Order 13402)**
   1. ***Section 1 Policy-*** Federal resources be used to deter, prevent, detect, investigate, proceed against, and prosecute unlawful use by persons of the identifying information of other persons
   2. ***Section 2 Identity Theft Task Force-*** The Task Force shall implement the policy set forth in section 1 of this order.

2. **The Presidents ID Theft Task Force made 31 recommendations**
   1. ***Recommendation 1.3-*** Require Federal Agencies to Review Use of SSNs
   2. ***Recommendation 3.1-*** Develop Concrete Guidance and Best Practices http://csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf
   3. ***Recommendation 3.2-*** Comply with Data Security Guidance
   4. ***Recommendation 3.3-*** Protect Portable Storage and Communication Devices

Key Privacy Performance Measures

Privacy Program Oversight	Is the appropriate oversight in place?
Privacy Impact Assessments	How many applicable systems have publicly posted PIAs?
Quality of Privacy Impact Assessment Process	What is the Inspectors General assessment of PIA process?
System of Records Notices	How many applicable systems with PII have SORNs?
Privacy-Related Policies and Plans	Are the privacy-related polices and plans in place?

New FY07 FISMA Reporting Requirements

Privacy-Related Policies and Plans

Are the privacy-related polices and plans in place?

- Privacy Attachments (4)
  - Breach notification policy
  - Implementation plan to eliminate unnecessary use of Social Security Numbers (SSN)
  - Implementation plan and progress update on review and reduction of holdings of personally identifiable information (PII)
  - Policy outlining rules of behavior and identifying consequences and corrective actions available for failure to follow these rules

OMB Memoranda Related to Privacy

- May 22, 2006, M-06-15, “Safeguarding Personally Identifiable Information”
- June 23, 2006, M-06-16, “Protection of Sensitive Agency Information”
- July 12, 2006, M-06-19, “Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments”
- September 20,2006, “Recommendations for Identity Theft Related Data Breach Notification”
- May 22, 2007, M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information.”
- January 18,2008, M-08-09 -- New FISMA Privacy Reporting Requirements for FY08

M-08-09 -- New FISMA Privacy Reporting Requirements for FY08

New requirements include:

- Number of each type of privacy review conducted by agency during the last FY;
- Information about the advice provided by the Senior Agency Official for Privacy (SAOP) during the last FY;
- The number of written complaints for each type of privacy issue allegation received by the SAOP during the last FY;
- The number of complaints referred to another agency for each type of privacy issue received by the SAOP on alleged privacy violations during the last FY.

Conclusion

Moving from “compliance “ to effective management and risk mitigation

Questions

For additional information, please visit www.egov.gov

John Lee
Acting Chief, Information Policy & Technology Branch, E-Gov/OIRA
Office of Management and Budget
725 17th Street NW
Washington DC 20503

(202) 395-3785