

# **Midwestern Intergovernmental Audit Forum**

---

## **Information Technology Security Update**

Lansing, MI  
September 4, 2008

---

---

## **Government IT Systems Face Increasing Risks and Threats**

---

- Government IT Systems are Inherently Risky:
  - Dollars passing through automated systems are rising
  - Increased complexity of systems
  - Preponderance of defective software
  - Availability of hacking tools/increased hacking
  - Reduced paper backup
  - Trend toward providing broad access
  - Controls critical infrastructure and operations

---

## Government IT Systems Face Increasing Risks and Threats

---

- Cyber Threats Are Evolving and Growing:
  - Unintentional
  - Intentional – Targeted and Nontargeted attacks
  - Sources of threats:
    - Criminal groups
    - Foreign nation states
    - Hackers and Hacktivists
    - Disgruntled insiders
    - Careless insiders

---

## **Government IT Systems Face Increasing Risks and Threats**

---

- Attack Vectors are Becoming More Sophisticated:
  - Spear Phishing
  - Defective Software
  - Web Applications
  - Wireless Computing
  - Global Supply Chain

---

## **Government IT Systems Face Increasing Risks and Threats**

---

- Impact of System Compromise Can Be Serious:
  - Modification or destruction of data
  - Loss of assets
  - Release of sensitive information (PII, law enforcement, homeland security, other)
  - Disruption of critical operations
  - Inappropriate use of computing resources

---

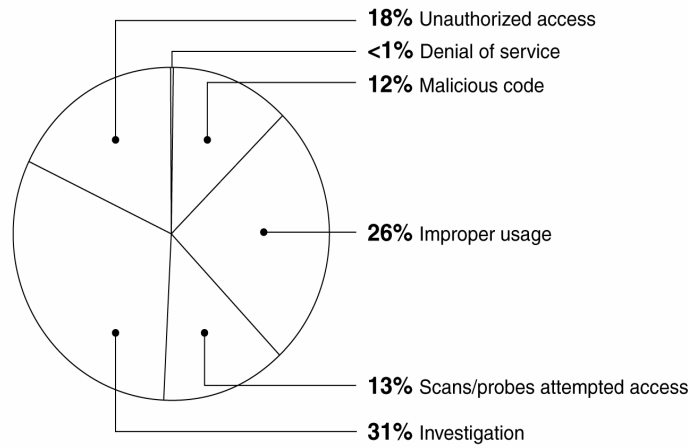
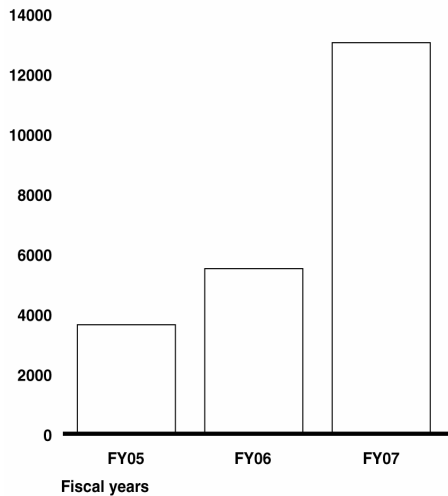
## Reported Security Incidents Are on the Rise

---

- Since January 2006, federal agencies have reported a spate of security incidents at risk, including the theft, loss, or improper disclosure of personally identifiable information on millions of Americans, thereby exposing them to loss of privacy and potential harm associated with identity theft.
- The number of security incidents reported by federal agencies to US-CERT has increased from about 3,600 to 13,000 from FY 05 to FY 07 (about a 259% increase)

# Reported Security Incidents Are on the Rise

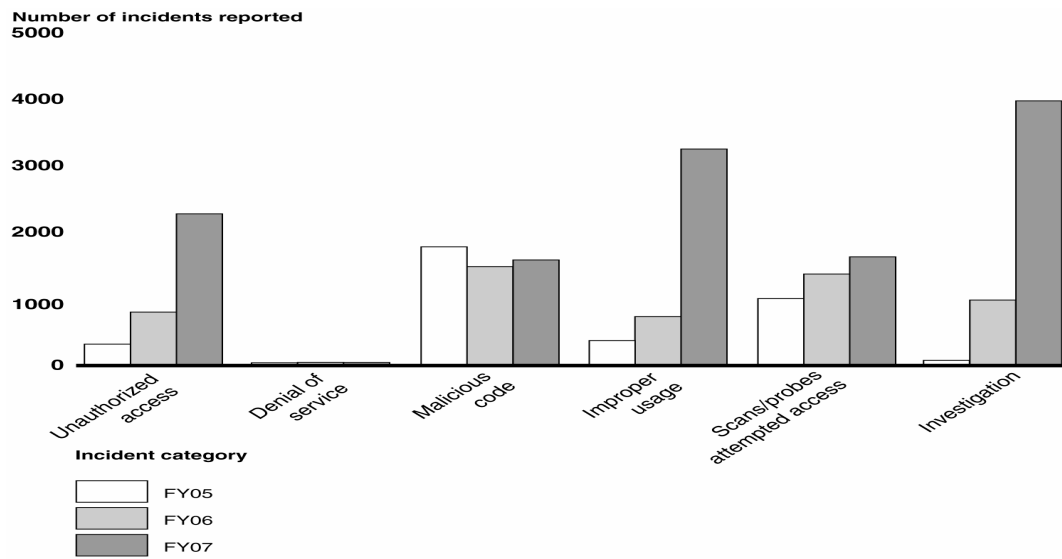
Number of incidents reported



Source: GAO analysis of US-CERT data.

Source: GAO analysis of US-CERT data.

# Reported Security Incidents Are on the Rise



Source: GAO analysis of US-CERT data.

---

## Federal Information Security Continues to be Weak

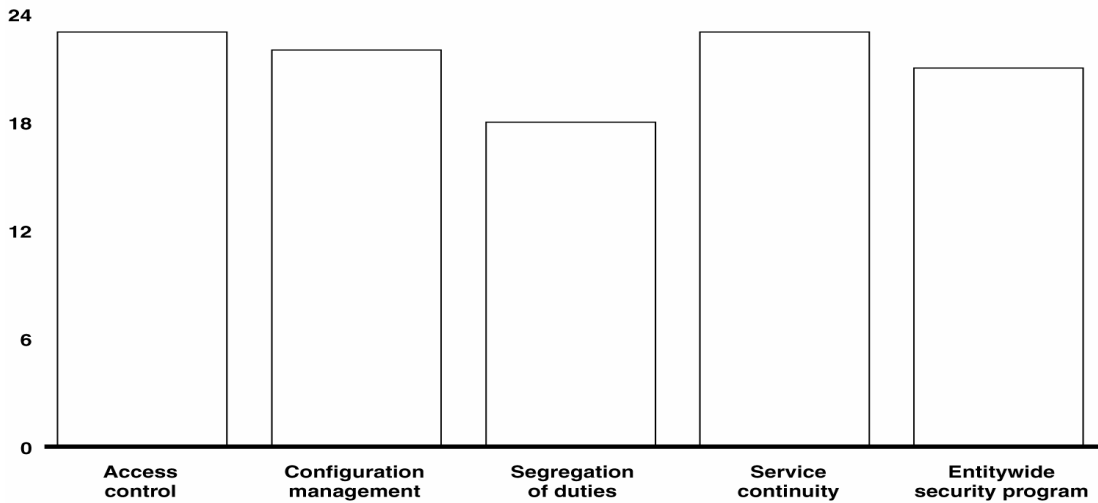
---

Significant weaknesses continue to threaten the confidentiality, integrity, and availability of federal systems and information at most major agencies:

- Most agencies have weaknesses in most control types
  - IGs cited IS as a “major management challenge” at 21 of 24 agencies
  - Auditors of agency financial statements reported that deficient IS controls were a significant deficiency or material weakness at 20 of 24 agencies
  - GAO has identified information security as a government-wide high risk area since 1997
-

## Federal Information Security Continues to be Weak

● Number of agencies



Source: GAO analysis of agency and IG reports for FY2007.

---

## Federal Information Security Continues to be Weak

---

- Agencies did not consistently:
  1. Identify and authenticate users to prevent unauthorized access
  2. Enforce the principle of least privilege
  3. Establish sufficient boundary protections
  4. Apply encryption to protect sensitive data
  5. Log, audit, and monitor security events
  6. Physically protect information assets

---

## **Federal Information Security Continues to be Weak**

---

- Nevertheless, federal agencies continue to report steady progress in implementing key IS requirements.
- Primary Reason for Inconsistency: OMB established security metrics that measure compliance not effectiveness

---

## **Auditors May Examine IT Security Controls In Several Ways**

---

- Audit of agency financial statements
- Annual independent evaluation required by FISMA
- Performance audits
- Post incident investigations and forensics

---

## **FISCAM Provides an Efficient Method for Examining IT Security Controls**

---

- Federal Information System Controls Audit Manual (FISCAM):
  - Consistent with GAGAS and FAM, including planning, testing, and reporting phases
  - Top-down, Risk-based approach
  - Draws on previous IS audit experience
  - Currently under revision – available at <http://www.gao.gov/new.items/d081029g.pdf>

---

## **FISCAM Provides an Efficient Method for Examining IT Security Controls**

---

- Chapter 1 – Introduction
  - Nature of IS controls, determining audit procedures, and legislative reforms
- Chapter 2 – Performing the information security audit
  - Planning the IS audit, performing IS audit tests, reporting audit results

---

## **FISCAM Provides an Efficient Method for Examining IT Security Controls**

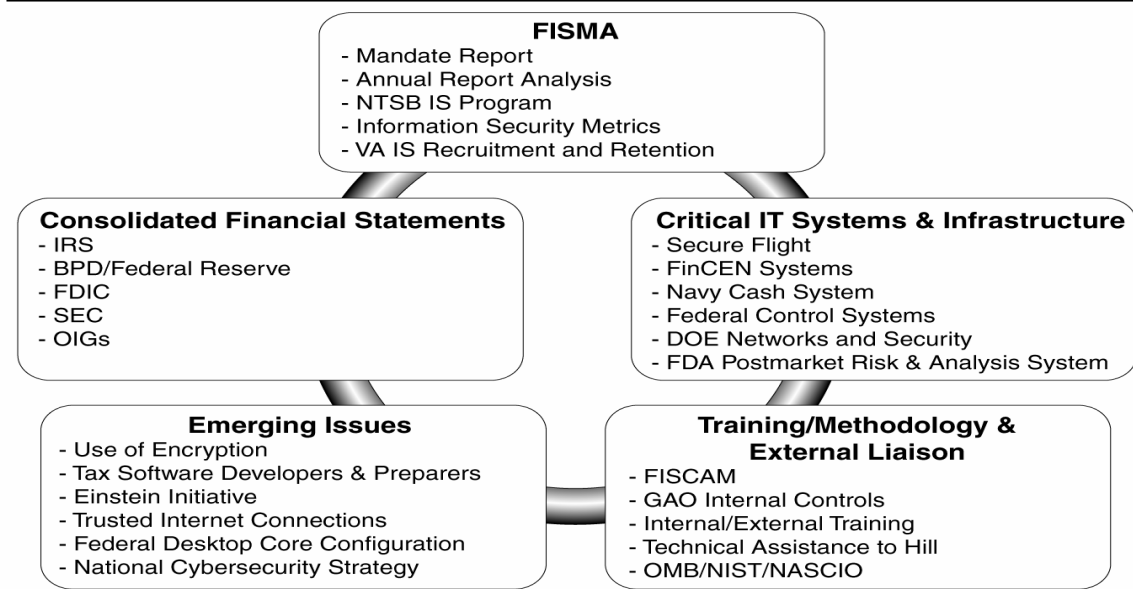
---

- Chapters 3 & 4 General and Application Controls
  - Describe broad control areas
  - Identify critical elements of each control area and related control activities
  - List common types of control techniques
  - List suggested audit procedures

# FISCAM Provides an Efficient Method for Examining IT Security Controls

Control Areas	Entitywide/ Component Level	System Level			Business Process Application Level
		Network	Operating Systems	Infrastructure Applications	
Security Management	—————▶				
Access Controls	—————▶				
Configuration Management	—————▶				
Segregation of Duties	—————▶				
Contingency Planning	—————▶				
Business Process Interface Data Mgmt.	—————			—————▶	

# GAO IT Security Focus Areas



---

## Contact Information

---

Gregory C. Wilshusen  
Director, Information Security Issues  
[wilshuseng@gao.gov](mailto:wilshuseng@gao.gov) (202-512-6244)

GAO Web Site: [www.gao.gov](http://www.gao.gov)

# Questions and Answers