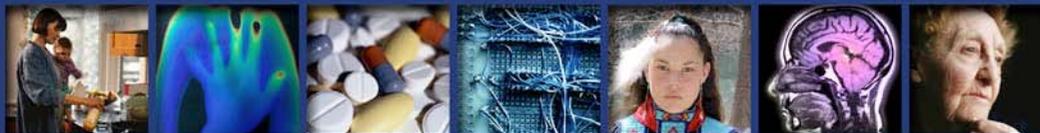




# Secure One HHS

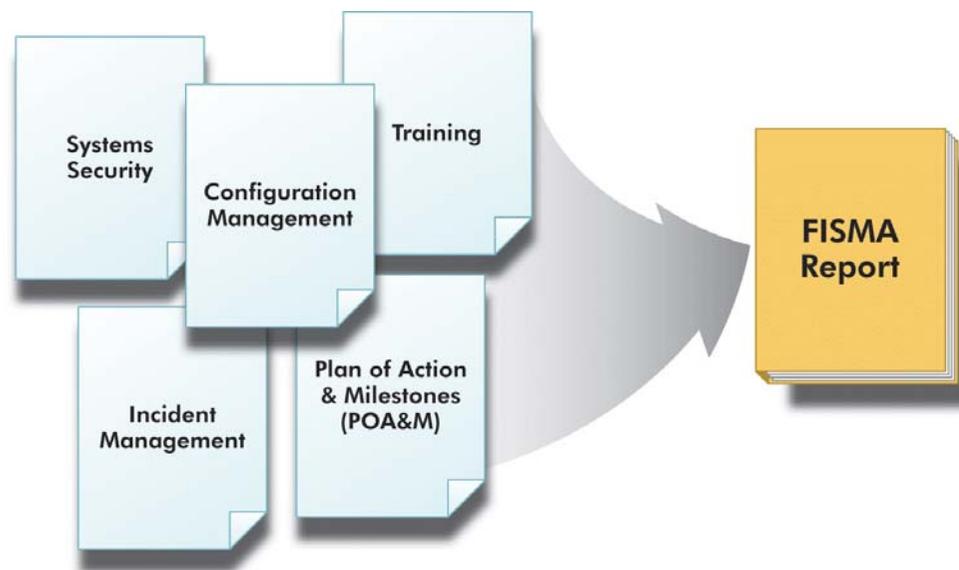
## Measuring Information Security and FISMA Compliance

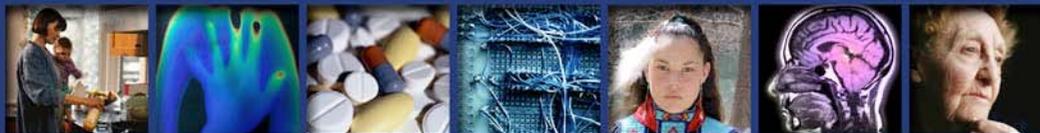




## While current FISMA metrics measure some key IT security components, they do not accurately reflect an Agency's comprehensive IT security posture

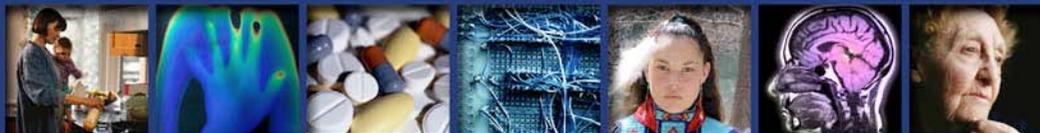
- ▶ Progress and the overall state of security should be estimated to mitigate vulnerabilities
- ▶ Resources should be devoted to standardize Inspector General evaluation methodologies
- ▶ Agencies should be required to report against performance metrics on a quarterly/annual basis to monitor progress
- ▶ Agency data should be used to populate standard dashboard templates for federal trending and distribution





## **FISMA metrics must support the integration of IT security into all Agency business processes**

- ▶ Provide information security protections commensurate with the risk and magnitude of potential harm
- ▶ Ensure information security management processes are integrated with agency strategic and operation planning processes
- ▶ Implement policies and procedures to cost-effectively reduce risks to an acceptable level
- ▶ Periodically test and evaluate information security controls and techniques
- ▶ Report annually on the adequacy and effectiveness of information security policies, procedures, and practices



## Metrics must also measure multiple facets of security program implementation

- ▶ Policy metrics – age of general information security policy, number of policies greater than three years old (older than FISMA)
  - Leading to the creation or update of policies
- ▶ Inventory metrics – age of data, frequency of update, etc.
  - Resulting in data calls and outreach, as necessary
- ▶ Process metrics – to assess the implementation of controls
  - Using NIST SP 800-53A (upon finalization) as a baseline
- ▶ Metrics on metrics – type and intent of additional metrics and/or oversight mechanisms in place
  - To determine effectiveness, necessity and compliance
- ▶ Monitoring metrics – type and frequency of network/system vulnerability scans, penetration tests, etc.
  - To formulate mitigation strategies, assign resources and ascertain real-time status reports
- ▶ Reporting metrics – timeliness, completeness and frequency of internal and external reporting, access to current and comprehensive data



# HHS Metrics Dashboard Concept

Inside this Community | Related Communities | Join this Community | Edit This Community

HHS Management Home Page | System Reporting Dashboards | Department-level Reports

Quick Links

- About Secure One HHS
- Tools
- Advisory Support
- Privacy
- Secure One Communications Center (SOCC)
- Education and Awareness
- HHS Initiatives
- Office of the Chief Information Officer (OCIO)
- HHS Office of Security and Drug Testing (OSDT)
- Physical Security

Contact Secure One Support

Contact the Secure One HHS help desk, Secure One Support (SOS), if you have any IT security questions or concerns. We can be reached via email at [SecureOne.HHS@hhs.gov](mailto:SecureOne.HHS@hhs.gov) or phone at 202-205-9581.

HHS SYSTEM REPORTING DASHBOARDS

**HHS Weaknesses Dashboard**  
This dashboard displays the total number of system weaknesses for the Department. All system weaknesses are assigned a system status and are separated accordingly.

**HHS Total Incidents Dashboard**  
This dashboard represents the total incidents reported by the Department for FY06.

**HHS Monthly Incidents Dashboard**  
This dashboard represents the type of incidents that have been reported for the Department during the month of August.

**HHS Monthly Event Summary Dashboard**  
This dashboard represents the type of events that have been reported during the month of August.

Click on the dashboards to view the detailed information.

HHS Weaknesses

HHS Weaknesses by Category

Category	Percentage
Critical	42%
High	31%
Low	27%

HHS Incidents by Type

HHS Incidents by type

Type Report	Number
Access Control	18
Denial of Service	12
Malware	10
Phishing	8
Spam	5
Unwanted Software	4
Other	3

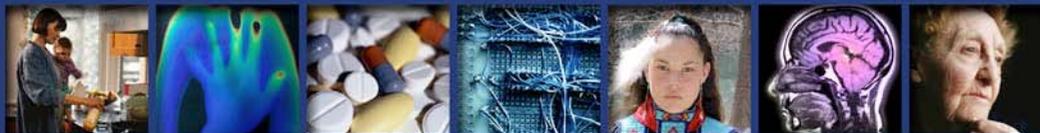
HHS Monthly Incidents By Type

HHS Monthly Incidents by type

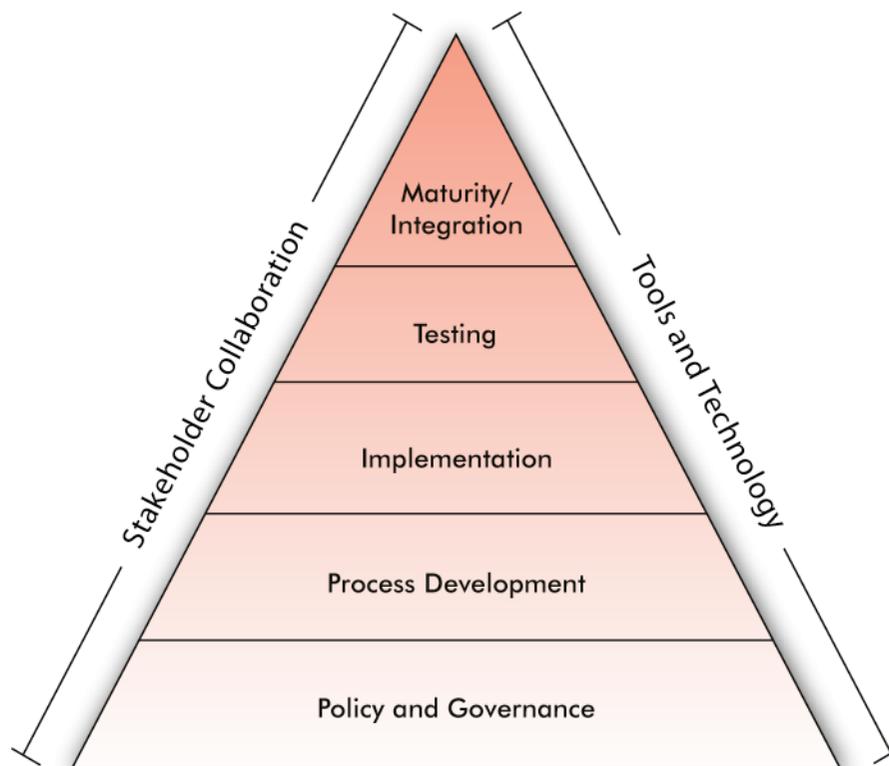
Type Report	Number
Access Control	18
Denial of Service	12
Malware	10
Phishing	8
Spam	5
Unwanted Software	4
Other	3

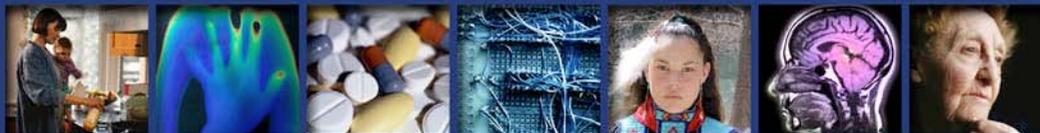
HHS Monthly Event Summary

HHS Events by type



## Ultimately, FISMA should measure overall progress towards IT security program maturity





**SECURE  
ONE HHS**

KEEP AMERICA'S  
HEALTH AND HUMAN  
SERVICES SECURE

**SECURE  
ONE HHS**

**KEEP AMERICA'S  
HEALTH AND HUMAN  
SERVICES SECURE**

**Secure One Support  
Secureone.hhs@hhs.gov  
202-205-9581**