



*OMB Update for the  
Information Security and Privacy Advisory Board*

*FISMA: Present Priorities*

*Carol Bales*

*Office of Management and Budget*

February 13, 2013



# Priorities for Protecting Federal Networks

*The Administration identified cybersecurity (Continuous Monitoring, Trusted Internet Connections/Einstein, and HSPD-12) as a Cross Agency Priority (CAP) goal.*

*The current status of agency progress and plans for improvement in these capability areas were shared with the President's Management Council and are reported quarterly on Performance.gov to ensure continuous visibility and to emphasize their priority for implementation at the agency level.*

*Additionally, the Federal CIO agenda focuses on three main themes: innovation, maximizing return on investment, and cybersecurity.*



# Priorities for Protecting Federal Networks

- **Continuous Monitoring**
  - **Goal:** Determine if deployed security controls remain effective over time in light of the inevitable hardware and software changes that occur.
  - **Objective:** Transform a static security control assessment and risk determination process into a dynamic system that provides essential, near-real-time, security-status-related information.
  - **Result:** Be able to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding network operations.
- **Trusted Internet Connections (TIC)**
  - **Goal:** Improve the Federal Government's network security posture.
  - **Objective:** Consolidate external internet connections
  - **Result:** Enhanced monitoring and situational awareness of all external network connections. Enhanced detection and intrusion prevention capabilities against cyber attacks.



# Priorities for Protecting Federal Networks

- **Authentication – HSPD 12**
  - **Goal:** Establish consistent, logical access control policy for federal computer networks.
  - **Objective:** Implement HSPD-12, which requires agencies to follow specific standards and processes for using Federal Personal Identity Verification (PIV) smartcard credentials. PIV cards will be used pursuant to standardized background investigations to verify employees' and contractors' identities, and enable network authentication while reducing duplication.
  - **Result:** Robust, multi-factor authentication, digital signature, and encryption capabilities on all federal networks.
- **When fully implemented, these priorities (Continuous Monitoring, Trusted Internet Connections, and HSPD-12) will provide a robust, risk managed defense of federal civilian networks.**



# FY13 FISMA CAP Goal Metrics

Administration Performance Area	Section	Performance Metric	Agency Minimal Level for 2013	Agency Target Level for 2013
Continuous Monitoring - Assets	2.2	% of assets in 2.1, where an automated capability (device discovery process) provides visibility at the organization's enterprise level into asset inventory information for all hardware assets.	80%	95%
Continuous Monitoring - Configurations	3.13	% of the applicable hardware assets (per question 2.1), of each kind of operating system software in 3.1, has an automated capability to identify deviations from the approved configuration baselines identified in 3.1.1 and provide visibility at the organization's enterprise level.		
Continuous Monitoring - Vulnerabilities	4.2	% of hardware assets identified in section 2.1 that are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level.		
Identity Management HSPD-12	5.2.5, 5.4.5 & 10.2.5	% of ALL people required to use Personal Identity Verification (PIV) Card to authenticate.	50%	75%
Boundary Protection CNCI #1	7.2	% of external network traffic passing through a Trusted Internet Connection (TIC). Not applicable to Department of Defense (DOD).	80%	95%
Boundary Protection CNCI #1 & #2	7.1	% of required TIC capabilities implemented by TIC(s) used by the organization.	95%	100%



# Current activities to support priorities

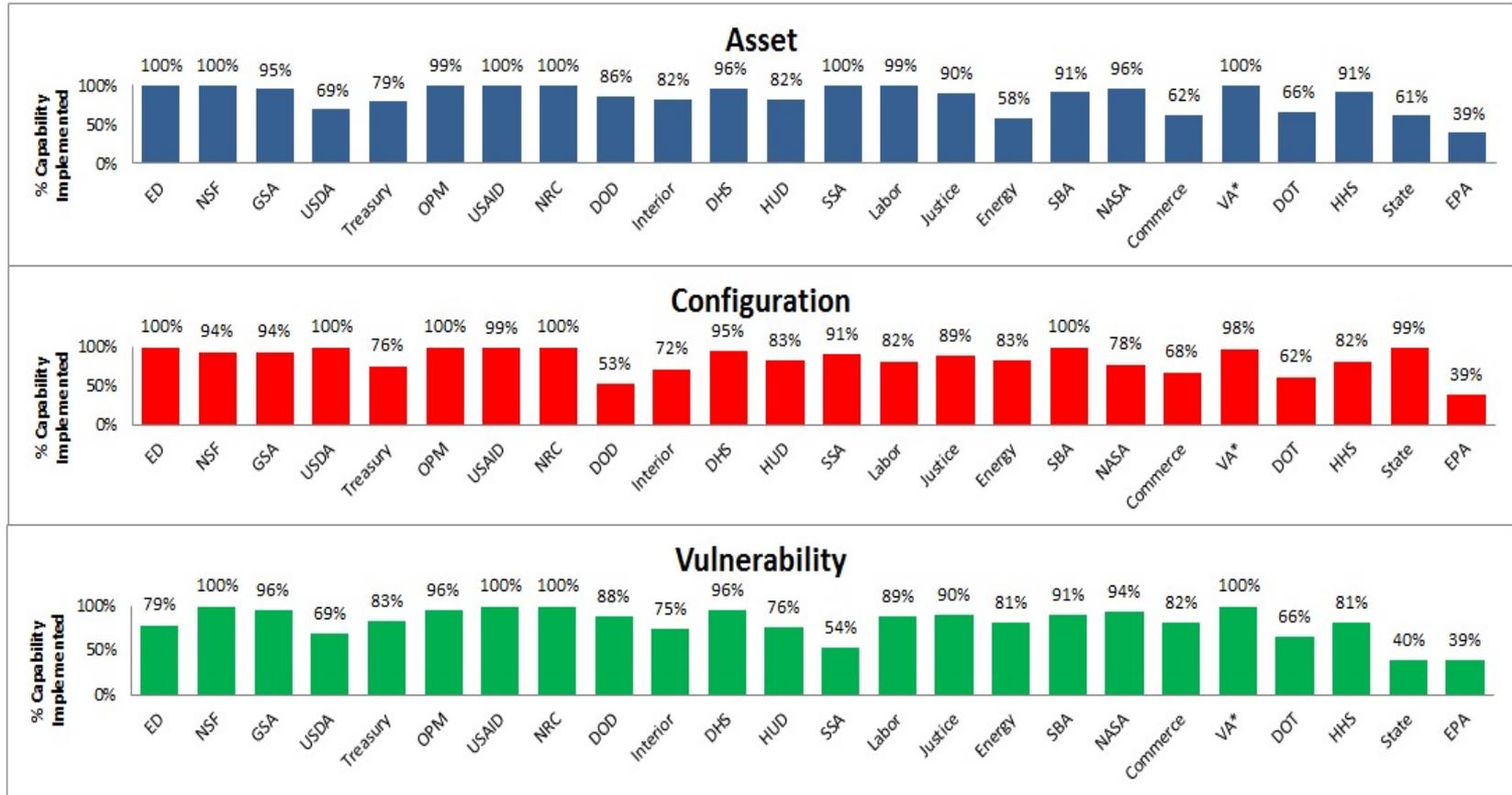
- In late 2012, DHS released a RFP to offer continuous monitoring sensors, diagnosis, mitigation tools and services to agencies
- In 2013, DHS and interagency groups to develop TIC 2.1 reference architecture focusing on mobile computing and cloud services
- FIPS 201-2 (revised HSPD-12 standard) to be issued
  - Addresses integration of the PIV card with mobile devices (includes option for alternative credential form factors for mobile devices)
  - Makes mandatory the digital signature and encryption certificates
  - Scheduled for Spring 2013 release
- NIST has begun work on SP 800-157, *Guidelines for Personal Identity Verification (PIV) Derived Credentials*
- Circular A-130 Appendix III review
  - Determine extent to which A-130 definitions, requirements and responsibilities may need to be updated
- DHS to continue hosting CyberStat accountability sessions
- OMB to continue PortfolioStat sessions to identify duplicative IT investments



# Background slides



# Percentage of Continuous Monitoring Capabilities Reported by Agencies



Continuous Monitoring Capabilities data as of Q4 FY2012.

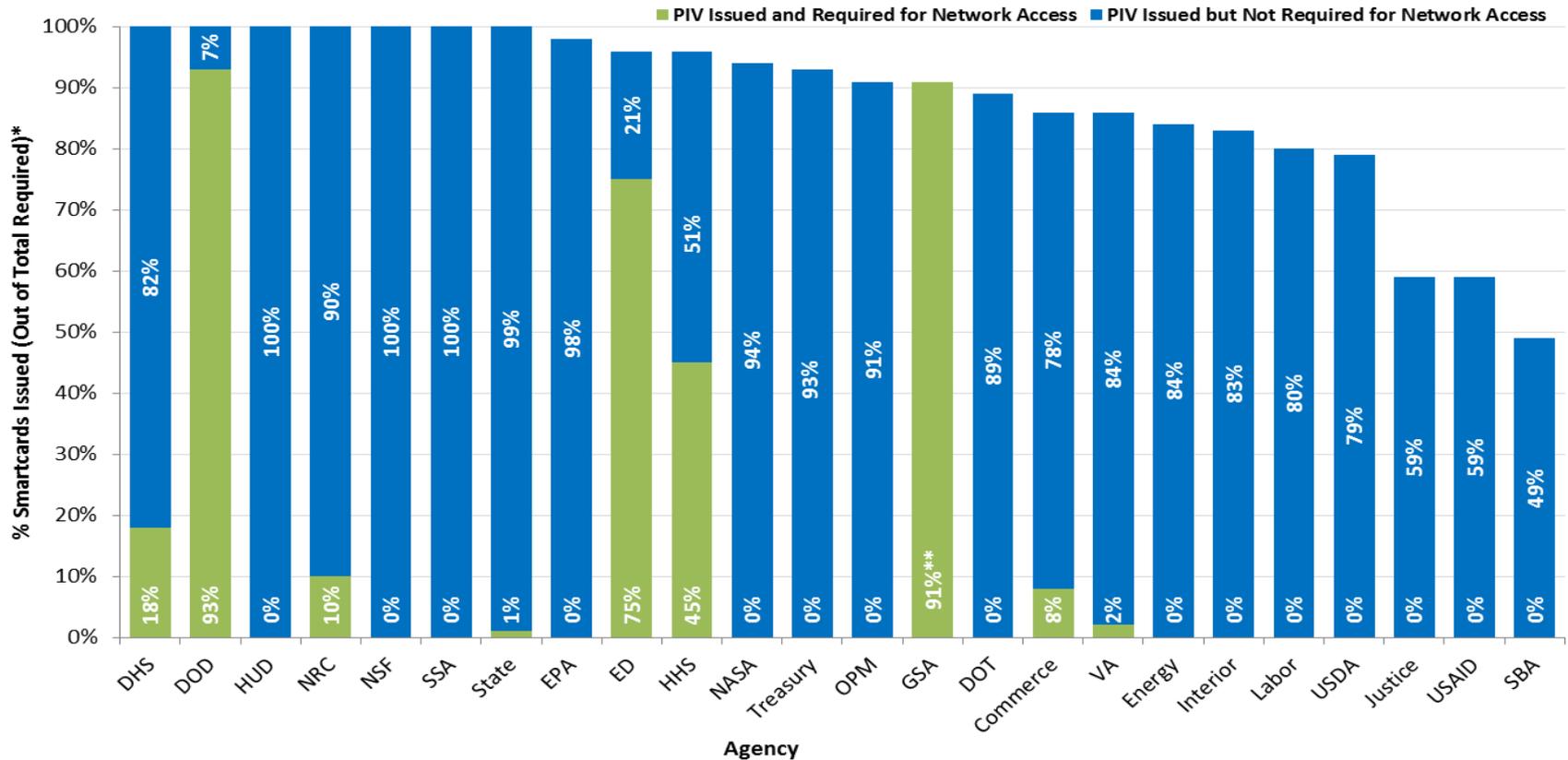
Asset –Agency FY13 target is 95%; Government-wide status is 86% (Increased 6% from Q4FY11)

Configuration –Agency FY13 target is 95%; Government-wide status is 70% (Decreased 8% from Q4FY11)

Vulnerability –Agency FY13 target is 95%; Government-wide status is 83% (Increased 3% from Q4FY11)



# Smartcard Issuance Progress and Percentage of User Accounts Requiring Use of PIV Cards for Network Access



\*All PIV card issuance percentages are from September 2012, and PIV card usage percentages are from November 2012

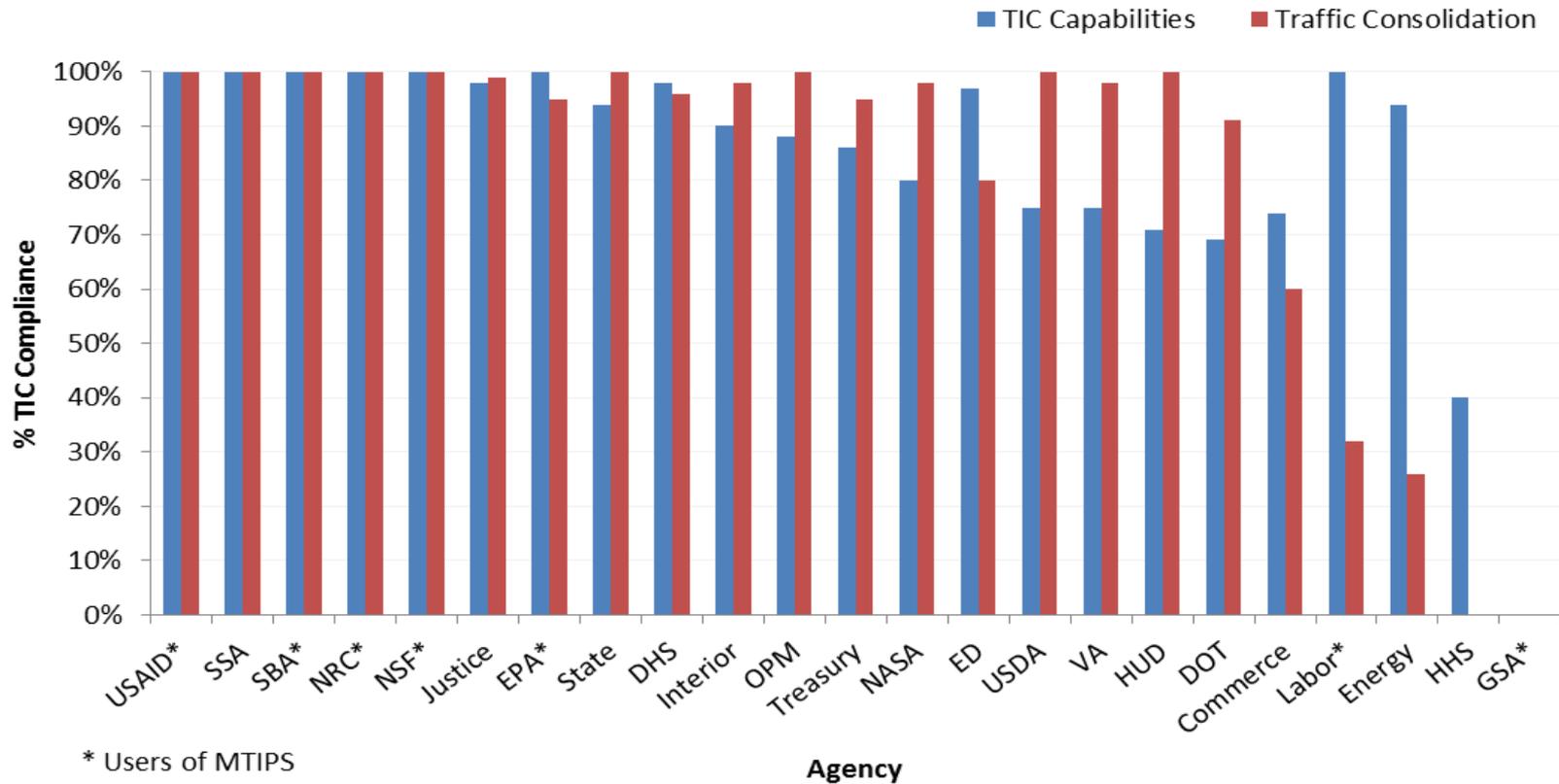
\*\*GSA reported 79% PIV card issuance and 92% PIV card usage for network access

**PIV Cards Issued as of September 1, 2012: 5,285,036 (96%)**

**Percentage of accounts requiring use of PIV cards for network logon: 57%**



# Percentage of TIC Security Capabilities and Traffic Consolidation Implemented by Agencies



TIC Capabilities: Agency FY13 target is 100%; Government-wide status is 81% (increased 12% from Q4FY11 to Q4FY12)

TIC Traffic Consolidation: Agency FY13 target is 95%; Government-wide status is 84% (increased 16% from Q4FY11 to Q4FY12)



**Carol Bales**

Office of Management and Budget

Executive Office of The President

[carol\\_bales@omb.eop.gov](mailto:carol_bales@omb.eop.gov)

202-395-9915