Federal Cybersecurity: The Start of the Marathon

OMB Cyber and National Security Unit

October 21, 2015

OMB Cyber Vision and Mission

- **<u>Vision</u>**: Reduce the number of cyber incidents where sensitive government information is compromised.

- **<u>Mission</u>**: Strengthen Federal cybersecurity through:

  1) Data-driven, risk-based oversight of agency and government-wide cybersecurity programs;

  2) Issuance and implementation of Federal policies consistent with emerging technologies and evolving cyber threats; and

  3) Oversight of the government-wide response to major cyber incidents and vulnerabilities to ensure appropriate mitigation measures are effectively implemented.

Agenda

- FY 2015 - Year in Review
- Cybersecurity Sprint Highlights
- Cybersecurity Strategy and Implementation Plan (CSIP)
- Upcoming Policies
- Questions

FY 2015 - Year in Review

- OMB Cyber and National Security Unit

- 14 CyberStats in FY 2015

- FISMA 2014

- DHS Binding Operational Directive on Critical Vulnerabilities

- Major Incidents

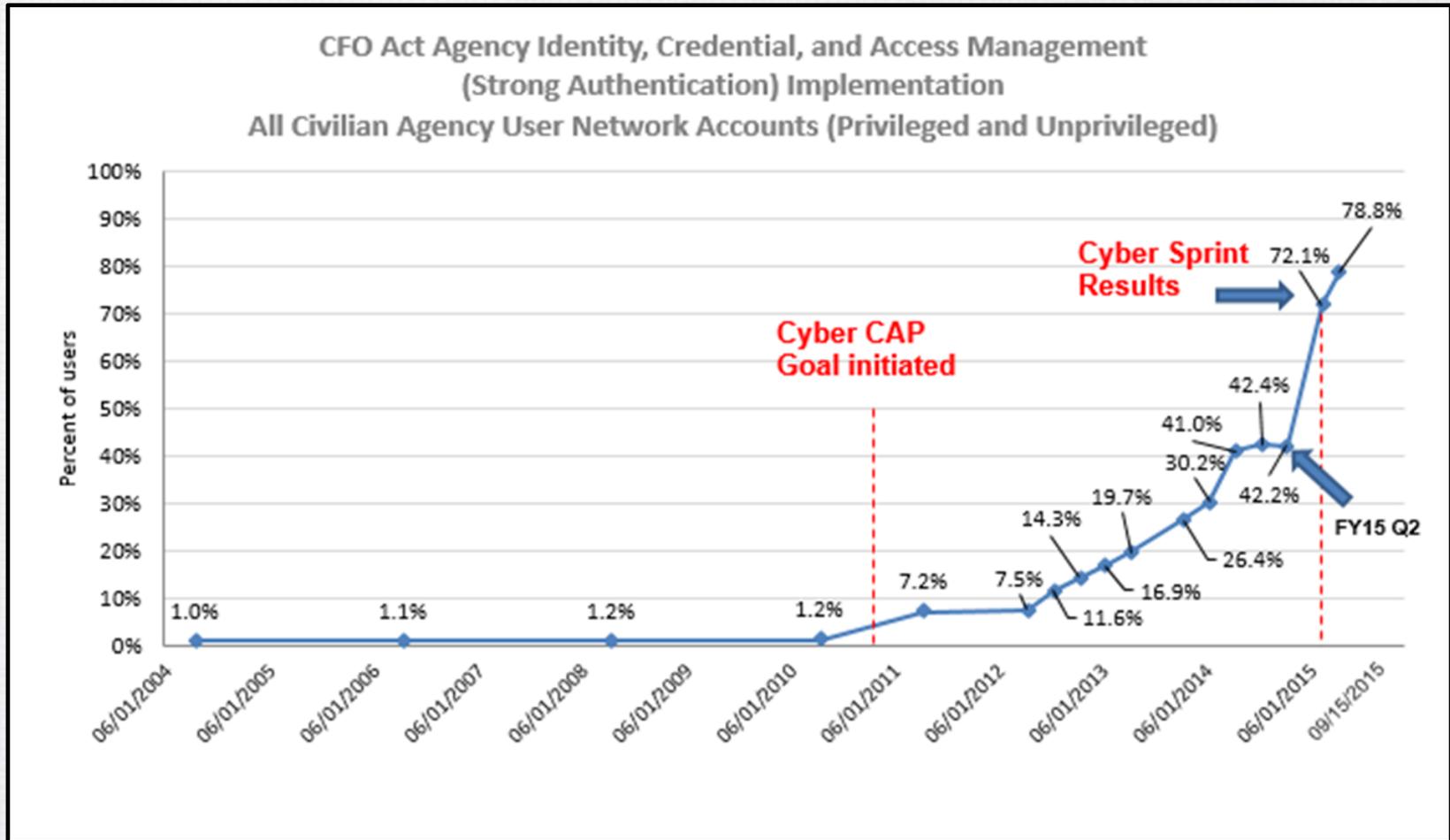- Cybersecurity Sprint

- Now What?

Cybersecurity Sprint

- Scan networks for Indicators of Compromise (IOCs)
- Patch critical vulnerabilities without delay
- Tighten policies and practices for privileged users
- Implement Personal Identity Verification (PIV) cards for network access, especially for privileged users
- Identify high value assets and review corresponding security protections

Strong Authentication

CFO Act Agency Identity, Credential, and Access Management (Strong Authentication) Implementation — All Civilian Agency User Network Accounts (Privileged and Unprivileged)

Source: Agency reported information

Cybersecurity Strategy and Implementation Plan (CSIP)

- **Prioritized Identification** and **Protection** of high-value information and assets

- **Timely Detection** and **Rapid Response** to cyber threats

- **Rapid Recovery** from incidents when they occur and accelerated adoption of lessons learned from these events

- **Recruitment** and **Retention** of the most highly-qualified cybersecurity workforce talent the Federal government can bring to bear

- **Efficient and Effective Acquisition** and **Deployment** of **Existing** and **Emerging Technology**

Upcoming Policies

- Cybersecurity Strategy and Implementation Plan (CSIP)

- FY 2016 FISMA Guidance

- Improving Cybersecurity Protections in Federal Acquisitions

- Circular A-130

Questions?