Achieving Compliance with OMB M-07-11

U.S. Department of the Interior

January 24, 2008

DOI IT Governance Model

- 13 Bureaus and Offices
- IT Management Council (ITMC) comprised of Bureau CIOs
- Chief Technology Officers Council (CTOC) comprised of Bureau CTOs
- IT Security Team (ITST) comprised of Bureau IT Security Officers

Overall Strategy

- Convened joint CTO/IT Security Officer offsite meeting to develop DOI's plan
- Plan briefed and accepted by CIOs
- Plan submitted to OMB on May 1, 2007
- Established small (5-6 person) working team with technical expertise in Windows, Active Directory, etc.
- Regular communication from working team to all governance bodies regarding findings and recommendations

Technical Approach

- Deferred Vista considerations for now
  - DOI not yet deploying Vista
  - Compliance with FDCC for Vista to be addressed as part of DOI Vista migration strategy
- Review NIST 800-68 and FDCC settings
  - Compared to existing bureau configurations
  - Testing in bureau environments to determine current level of compliance
  - Relatively small number of deviations identified
  - Ensure compliance with existing DOI policy
- Leverage existing POAM process for identifying deviations and tracking resolution status
- Ongoing communications with governance bodies
- Buy-in from CIOs on version 1.0 of Baseline XP STIG

Policy Issuance

- Formally defined requirement for bureaus to meet or exceed DOI Baseline XP STIG by February 1, 2008
  - Distributed INF file with settings
  - Stronger settings encouraged
- Formally defined PO&AM process to track deviations

Lessons Learned

- Get executive buy-in
- Ensure compliance with existing policies
- Recognize compliance will not be achieved overnight
- Communicate, communicate, communicate