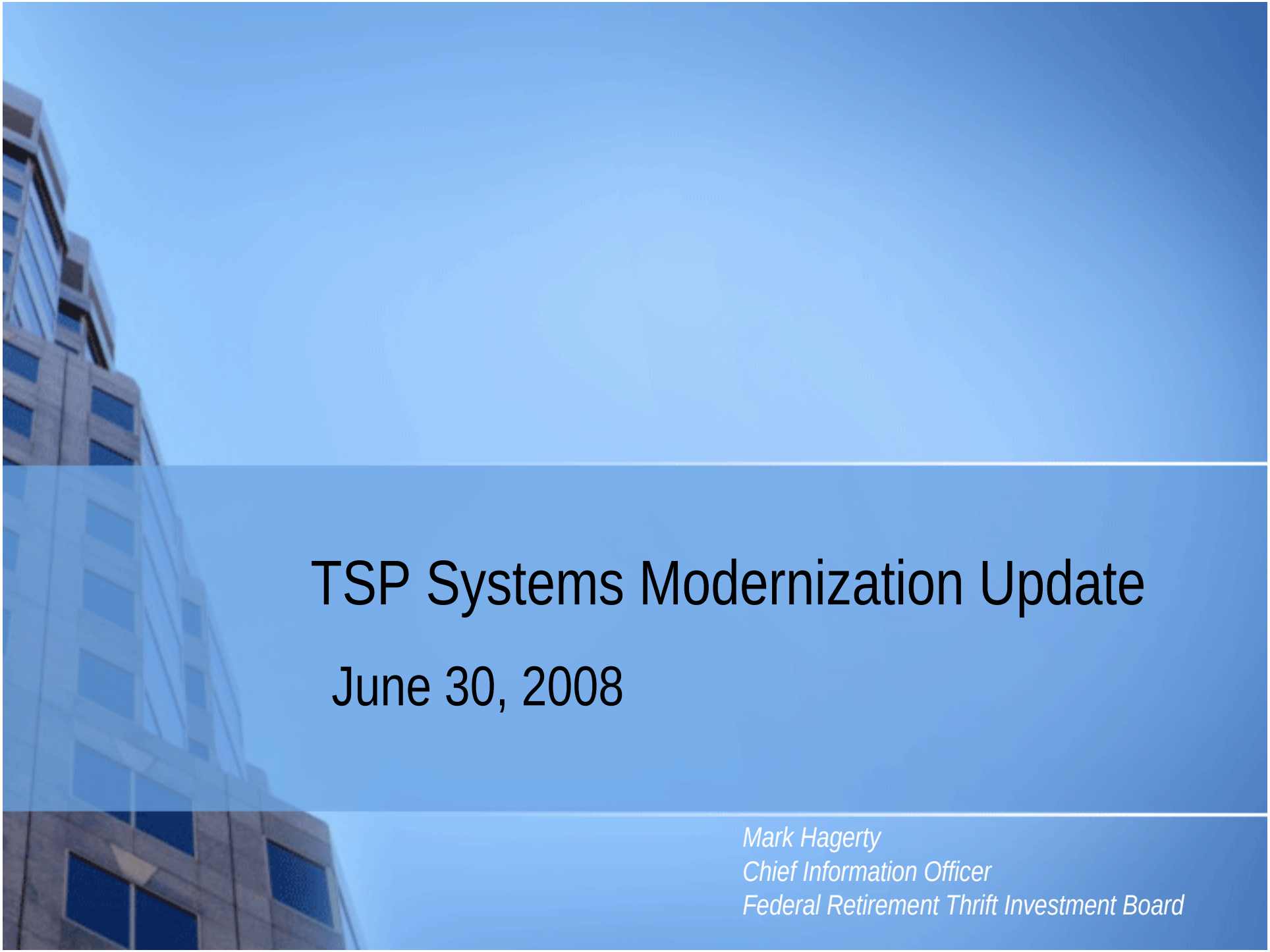


TSP Systems Modernization Update

June 30, 2008

Mark Hagerty
Chief Information Officer
Federal Retirement Thrift Investment Board

Background

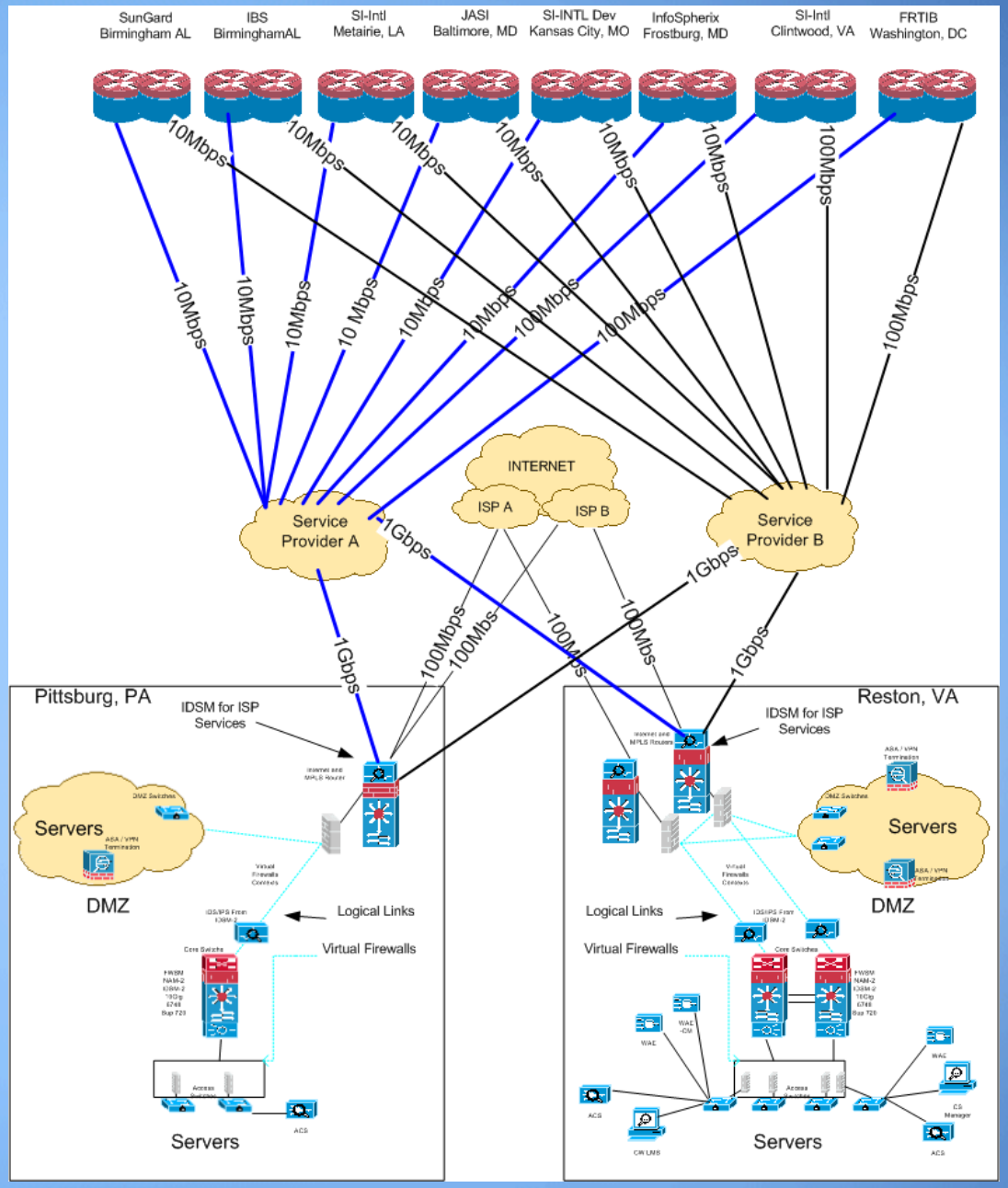
- Significant changes in TSP kept focus on current state:
  - Change to Daily valued plan
  - Moved data center from NFC
  - Established backup data center
  - Established parallel call centers
  - Outsourced business operations
  - …and that hurricane thing
- Time to focus on moving the technology and services forward

TSP Modernization Objectives

- Business Assurance: *Purposeful Survival*
  - Establish the capability to support TSP functions and systems that, based on an unpredictable scenario:
    - *Survive* emergencies, natural disasters, cyber attacks or accidents,
    - Are *robust and adaptable* enough to continue delivery of most important TSP products and services,
    - Have *sufficient, on-demand capacity* to ensure critical processes can be performed in a timely manner in the event of a significant market event, and
    - Ensure the *safety* and *security* of TSP data, assets and people

Deliver ***critical*** TSP services no matter what…

The "*Business Assured*" architecture



Laying the Ground Work

- Completed a comprehensive engineering review of the TSP technology infrastructure, including:
  - Mainframes
  - Storage subsystems
  - Server environment
  - Network
  - Security
  - Quality Assurance and Configuration Management

Mainframes

- Existing mainframes did not have sufficient processing capacity or memory, and were no longer upgradable.
- Solution
  - Replace both mainframes with newer technology; more memory, faster processors
- Status
  - Mainframes were procured in FY07 and installed in Q1 FY08, and are currently supporting both our primary and backup data centers.
- Effort Remaining
  - Turn on additional processors (FY08/Q4)
  - Implement full end-to-end MF test environment (FY09/Q2)

Storage Subsystems

- Storage subsystems quickly nearing capacity and (floor) space limitations. Devices were slow by today's standards, and data housed across multiple device types
- Solution
  - Replace storage subsystems in Reston and Pittsburgh with high-speed, scalable solution. Eliminate direct-attached storage
- Status
  - Purchased and installed initial phase of enterprise storage area network (SAN)
- Effort Remaining
  - Procure and implement remaining Opens Systems storage capacity (FY08/Q3)
  - Procure and implement mainframe storage solution (FY09/Q1)

Servers

- Server environment included too many “point solution” devices with direct attached storage, most would be end-of-lifecycle by FY08 end.
  - Solution
    - Consolidate and replace servers in both Reston and Pittsburgh with new virtual server technology, which is scalable, and configured for redundancy and high availability.
    - Include a test environment for application testing
  - Status
    - Completed engineering design
  - Effort Remaining
    - Identify and execute Phase 1 procurements (FY08/Q3)
    - Identify and execute Phase 2 procurements (FY09/Q1)
    - Server consolidation implementation (FY08/Q4 – FY09/Q4)

Network

- Existing network equipment did not support IPV6, inadequate redundancy in some areas, and many components reaching end-of-lifecycle.
  - Solution
    - As part of transition to IPv6, eliminate all single points of failure associated with critical network hardware and paths.
    - Proactively monitor/manage the TSP network and servers with appropriate tool sets to ensure fast problem recognition and resolution
  - Status
    - Network monitoring software selected and procured
    - Draft network design complete – pending final review to ensure it meets SCON requirements
    - Draft Statement of Objectives for telecommunications circuits completed and pending procurement review and release
  - Effort Remaining
    - Begin implementation of network monitoring tools (FY08/Q3)
    - Identify and procure network hardware (FY08/Q3)
    - Implement Network and Telecommunications redesign (FY08/Q3 – FY09/Q4)

Security

- Findings
  - Firewalls, intrusion detection, antivirus all in place, but building redundant capabilities is prudent.
  - All data “in motion” encrypted.
  - Additional emphasis required on network vulnerabilities
- Solution
  - Greater emphasis in IT Security program needed
- Status
  - Change to new storage area network should include encrypting data at rest.
  - Account numbers implemented Oct. 2007
  - Hired CISSP to oversee FRTIB IT Security Program
  - Implement customizable USER ID
  - Hire additional contractor IT security personnel
  - Quarterly penetration tests at all FRTIB locations
- Effort Remaining
  - Procurements in progress for:
    - Fraud Detection and Mitigation software
    - “Brand Monitoring” and Anti-Phishing service
    - Social Engineering (Testing, Review, and Training)

Quality Assurance and Configuration Management

- Findings
  - Improved QA processes require additional processing power
  - QA and CM initiatives need to be integrated into operations environment
  - End-to-end, functional test area needed
  - Additional staff needed to oversee QA/CM program initiatives
- Status
  - Hired QA/CM lead to address Government roles and expectations/measures of contractor performance
  - Installed CM software tools for mainframe and distributed applications to control code access/changes
  - Installed CM software tool on “frtib.gov” and “tsp.gov” web sites
- Effort Remaining
  - Complete system documentation effort; baseline for future changes and validation
  - Complete processes to assess software maintenance costs
  - Increase market research efforts to identify COTS solutions for new initiatives

Summary

- Project on schedule
- Working to clarify FY09+ budget impacts for remaining hardware and telecommunications costs, maintenance tails.