VARMINT

Vulnerability Assessment & Remediation Management INTegration

Phase I : Requirements Development

Using Prototype of Near-Continuous Configuration and Security Patch Vulnerability Detection and Monitoring

June 30, 2004

Agenda

1. **Objectives**
   1. Ultimate
   2. Today's
2. **Technical Requirements & Logistics**
3. **Timeline and Goals**

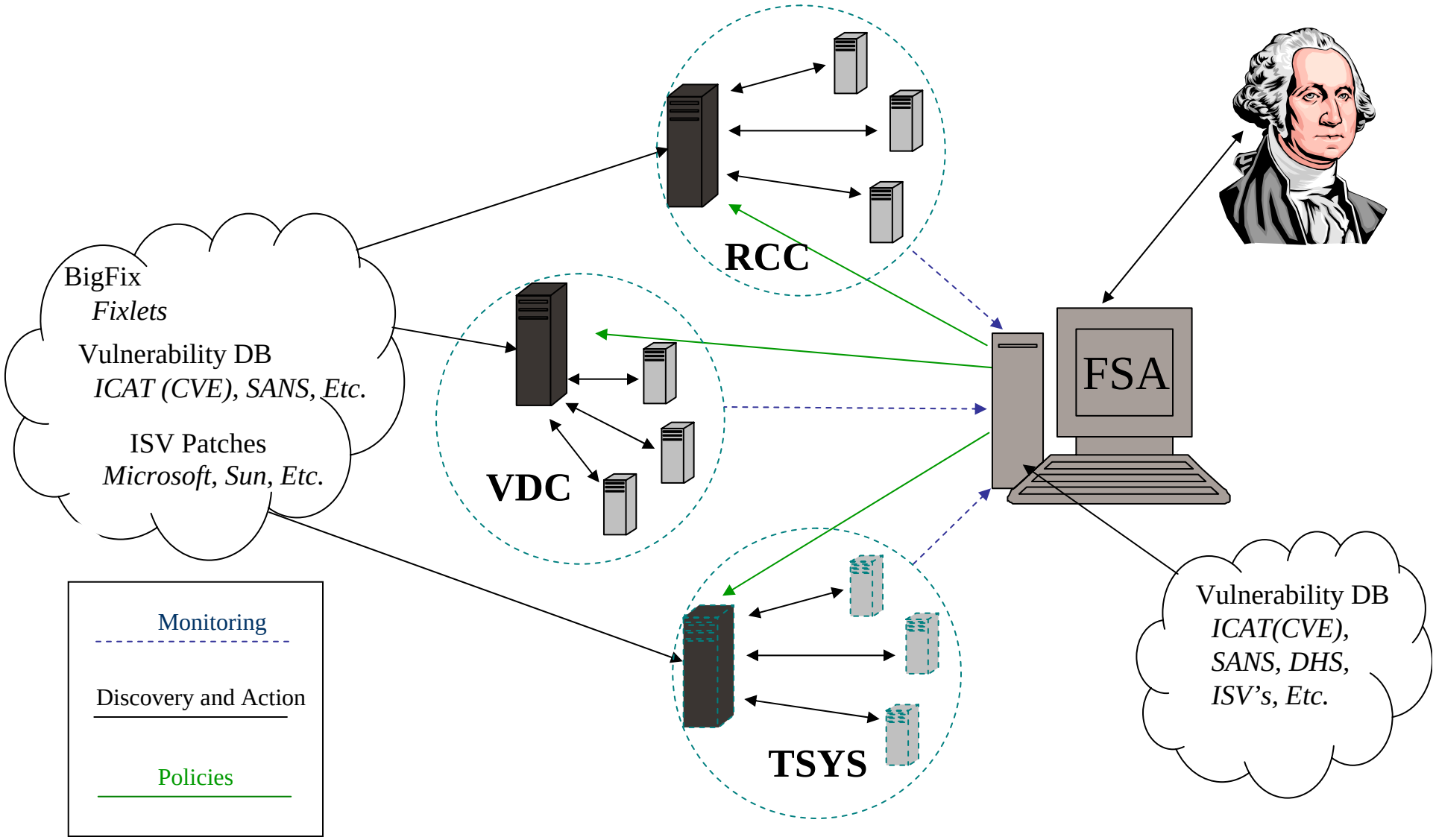
© 2004 BearingPoint, Inc.

Ultimate Objective

1. **Risk/Exposure Management**
   - Continuously know <u>what</u> assets need to be protected
   - Define <u>why</u> they should be protected and…
   - <u>How</u> they will be protected
2. **Develop and Standardize Policies To:**
   1. Ensure That FSA's tolerance for risk is understood across the enterprise
   2. Create effective communications path between FSA leadership charged with risk management, and IT administrators/implementers who operate network and systems on a day to day basis

© 2004 BearingPoint, Inc.

Ultimate Objective



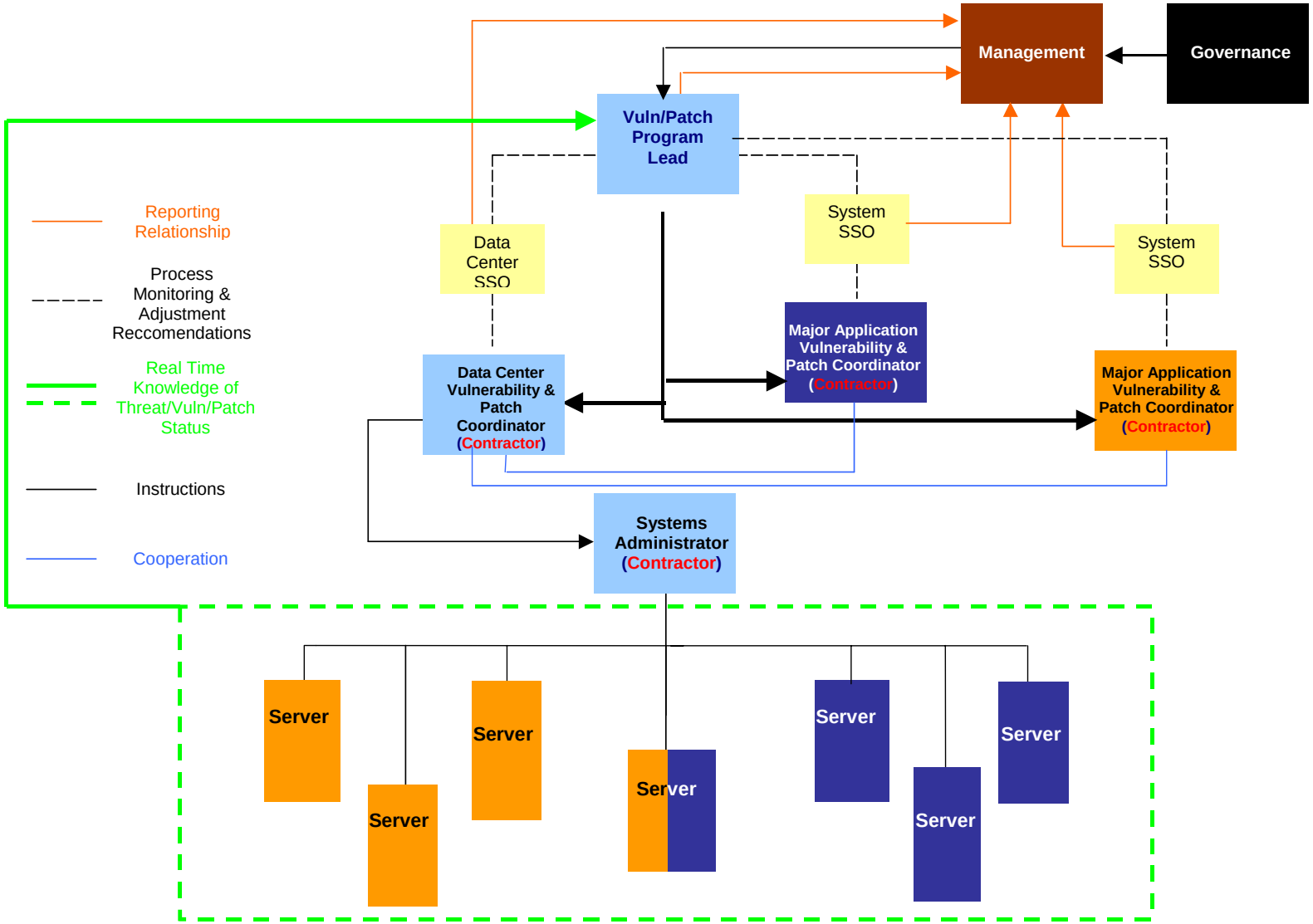
© 2004 BearingPoint, Inc.

Today's Objective

1. **Work with CSC to accommodate vulnerability detection and monitoring prototype that will allow FSA to:**
   1. Create workflow
   2. Select commercial tool(s)
   3. Develop Policies
2. **Discuss resources required**
3. **Discuss timeline**
4. **Discuss next steps**

© 2004 BearingPoint, Inc.

Tool Enabled Workflow



© 2004 BearingPoint, Inc.

Technical Requirements and Logistics

1. **Resources**
   - Hardware, Software
     - Big Fix Enterprise Server (BES), Console, Relay, Agents – 60 day trial
     - Underutilized Windows 2000 server at VDC
     - Sample of 10-30 servers at VDC – Solaris, Windows mix
     - Communications
   - Tasks
     - Install BES on FSA machine
     - Open communication path to relay and sample servers
     - Push agents and relay to machines
     - Validate Security
   - Personnel
     - FSA Security Administrator of Big Fix Enterprise Server and Console installed on machine
     - CSC, EdNet to facilitate opening communication path
     - FSA Security and Privacy Group Support

© 2004 BearingPoint, Inc.

Timeline

- **April/May-** Research of commercial solutions to accommodate the FSA environment was stepped up to include demonstrations from three vendors and research and teleconferences with several more. Other products continued to be evaluated. Devised map and overview of workflow
- **June –** Prepare logistics and select prototype for near real-time inventory, vulnerability, and remediation analysis tool
- **August/September–** Implement Prototype. Evaluate: Baseline; Define asset:threat classification schema; Define policies, policy, compliance, and accountability techniques and measures.

© 2004 BearingPoint, Inc.

END

Supporting Slides Follow…

© 2004 BearingPoint, Inc.

Requirements Development

Develop Requirements Using Near Continuous Monitoring of the Patch and Configuration:Vulnerability status of a sample of 10-30 servers in the VDC to:

- Formulate Workflow, Policy, Compliance, Accountability rules and techniques that consider criticality, impact, Federal law, ED policy, FSA policy and environment, testing, change management, personnel, other necessary resources and processes.
- Identify Most Suitable Commercial Tool(s)
- Determine best architecture for vulnerability management solution

© 2004 BearingPoint, Inc.

Prototype Tool: BigFix

Unique architecture designed to minimize strain on resources

Excellent discovery capability

Excellent UI

Can turn off deployment

Secure

Very Good Reporting

Open Prospects for future integration

© 2004 BearingPoint, Inc.

Current Climate

- **Comprehensive Integrated Vulnerability Management Program With Centralized Monitoring Is Recommended By Gartner (June 2004)**
- **Most components are required by FISMA**
- **Configuration/Patch Management a crucial component**
  - Just released GAO report on Patch Management
  - Recent Audit findings at FSA
  - Recent exploit incident at FSA
  - Recent attention in press to “need to know inventory” – Congressman Putnam

© 2004 BearingPoint, Inc.

Patch Management

First Step is to Know the "Current State" of the Environment & Develop Requirements

- **For Patch Management this means:**
  1. **Centralized knowledge of OS, APPs, Versions, Revisions, Patch "Level" or better term is, Patch "Status" in real-time or near real-time**
  2. **Up-to-date threat data from sources such as ICAT, SANS, MS – a vulnerability and remediation Advice database**
  3. **Best practices and asset classification data**
  4. **Automated deployment where needed (I.e., desktops)**

© 2004 BearingPoint, Inc.

Commercial Tools

Multiplatform Capable

- **PatchLink**
- **BigFix**
- **Marimba**
- **Symantec**
- **Eeye Digital**
- **Others**

© 2004 BearingPoint, Inc.

Gartner

Gartner says…

Enterprises that implement vulnerability management will experience 90 percent fewer successful attacks than those that only make an equal investment in intrusion detection systems.

© 2004 BearingPoint, Inc.

Gartner (Cont)

Gartner says…

Evolution of IT Security Management

- More intelligence about the classification, status and configuration of targeted resources
- Integration with network and system management information
- Embedded problem management workflow and integration with enterprise problem management systems
- Long-term archive and analytics
- Control and automated remediation

Gartner

© 2004 BearingPoint, Inc.

FISMA etc.

FISMA (and NIST, GAO, OMB) says…

"Agencies must maintain an inventory of major systems"

and goes on to say that,

"Such inventory shall be-- used to support information resources management, including-- monitoring, testing, and evaluation of information security controls."

GAO Report released last week says:

Common patch management practices—such as establishing and enforcing standardized patch management policies and procedures and **developing and maintaining a current technology inventory**—can help agencies establish an effective patch management program and, more generally, assist in improving an agency's overall security posture.

© 2004 BearingPoint, Inc.

Regulatory Trend

Gartner, FISMA, Audits, Recent Exploit, and Congressman Putnam says…

For competent security - Centralized, near-continuous, vulnerability monitoring and; automated, facilitated, and documented workflow and processes to classify, prioritize, and remediate are needed!

© 2004 BearingPoint, Inc.