



**Patch Management**  
*Outline of Requirements to move forward  
towards achieving a “Managed State”*

- I. Intro
  - A. Patch Management overview
  - B. Other Software Vulnerability Management (VM)
  - C. Effective and Comprehensive Total VM
    - 1. Discovery – ongoing, systematic
    - 2. Assessment – strong databases of patches/vulnerability signatures
    - 3. Recommended remediation and prevention measures
    - 4. Repair and Repair Tracking – Accountability
  - D. NIST Guidance Evolution
  
- II. Patch Management
  - A. Identify Software Patch Levels
  - B. Match Levels w/ Existing Vulnerabilities
  - C. Identify Any Alternate Remediation of Existing Vulnerabilities
  - D. Identify Any Valid or Perceived Valid Reasons for Non-Remediation
  - E. Identify Any Patch Management Process
  - F. Identify Any Automation Tools
  - G. Identify Any Operational Issues Research
  - H. Identify Testing Methods/Procedures
  - I. Identify Any Roles and Responsibilities
  - J. Identify Any Accountability Controls
  
- III. Vulnerability Assessment (Scanning) and Remediation
  - A. Identify Scanning Tool
  - B. Identify Schedule
  - C. Identify Findings Classification Criteria
  - D. Identify Outstanding Critical Vulnerability Findings
  - E. Identify Responsibility for Findings Remediation
  - F. Identify Accountability Controls for Remediation
  
- IV. Commentary on State of Patch and Vulnerability Management (By System and FSA-Wide)
  
- V. Show How Automation Solves Deficiencies
  
- VI. Compare Solutions
  
- VII. Discuss Future Requirements