

## FSA Vulnerability/Patch Management Proof of Concept Case

To comply with FISMA and competently ensure that software and configuration vulnerabilities in FSA's systems and major applications do not impact mission and business critical operations, the Security & Privacy Group recommends the following measures be undertaken immediately:

- Use available and proven technology to, at all times, know the inventory of all systems and network hardware settings and configurations, operating systems, OS versions and security patch status; applications, application versions and application security patch status.
- Use available and proven technology to efficiently and effectively assess any adverse impact on mission criticality, business criticality, and business operations that any configuration or unpatched software, in the current inventory, may enable.
- Use available and proven technology to prioritize and maximize efficiency and effectiveness in remediating current vulnerabilities
- Use available and proven technology to employ a workflow, communications, accountability, and reporting vehicle that ensures maximum effectiveness of the technology's utilization to improve security first, improve reporting second, and as a byproduct of the two, ensure compliance and reduce the depth and breadth of future audits.

**To accomplish the above, FSA wishes to, first, establish proof of the value of real-time knowledge of configuration and software vulnerabilities and to develop procedures and guidelines for remediation, based on this previously unavailable capability. Additionally, FSA will have the ability to better assess GSS contractor's patch and vulnerability management processes, which currently shows evidence of inadequacies.**

**The proof of concept is not designed to take any action. It is simply a discovery and detection of assets and assessment of asset status as measured against a current database of known vulnerabilities**

### Bases

The Security and Privacy Group has researched Federal law and guidance extensively and concluded that the FSA is responsible for implementing such a solution. Legislators and oversight bodies have recently begun to recognize this imperative and will, no doubt, amend their rules and guidance to more directly demand this type of solution. Evidence of this is as follows:

- Congressman Putnam of Florida, with his picture on the front cover Information Security Magazine, Federal Computer Week and Government Computer News in the past month, has sharply criticized federal IT security management for not knowing their inventory asking how agencies can know where they are vulnerable if they don't know what they have.
- FISMA states that 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." This wording seems to be originally constructed around scanning.
  - Periodic, disparate, scanning is repeatedly proving that it cannot accomplish the task of either compiling inventory or enabling effective and efficient remediation of critical vulnerabilities.
  - Scanning is an encumbrance on network bandwidth and thus incapable of providing real-time knowledge. In addition, scanning tools are destined for extinction in favor of host based or

“agent” discovery and remediation, as we deploy more (ultimately all) encrypted communications.

- Recent IG findings of software and configuration vulnerabilities in certain major applications
- Recent infection of servers with Sasser Worm at one major application

### **Phase I: Proof of Concept**

The FSA Security and Privacy Group has researched vulnerability and patch management methods, practices and commercial tools extensively - both currently used at FSA and in the general marketplace – and have devised a methodical process to achieve our goal of addressing this increasingly critical component of information security.

- We have developed a phased plan to implement the best tools and process. The first physical step towards successful implementation is a “proof of concept” using a trial version of a commercially available tool deployed and managed by FSA personnel with the assistance of BearingPoint.
- Our proof of concept will demonstrate the value of real-time knowledge of the patch and configuration vulnerability status of a sample of 15-30 servers in the VDC and to:
  - Develop workflow and accountability rules and techniques that consider criticality, impact, Federal law, ED policy, FSA policy and environment, testing, change management, and other processes.
  - Gather requirements for enterprise solution to deploy the best tool(s) to discover, detect, and remediate vulnerable software and configurations.
  - Work through any conflicts that may arise between FSA security requirements, as mandated by law, and any GSS contractual boundaries.
  - Demonstrate the value of transparency into the operations of GSS contractors for enhanced accountability and performance monitoring.
  - Provide GSS contractors with a centralized means of patch and vulnerability management that:
    - Is cost-effective because of economies of scale
    - Ensures consistency across contractors and better performance measuring opportunity.
    - Attracts rather than mandates its use

### **Other requirements gathering**

FSA Security and Privacy Group intends to seek out other business reasons for use of the inventory capability. For example, it could potentially allow contracting office to utilize this transparency to manage licensure and contract performance and for devising more appropriate, accurate and timely performance requirements for future contracts, especially with respect to security.

### **Implementation Requirements**

- Business Integration Group Approval
- Architecture Group Approval
- Major Application BO approval
- Contractor coordination to install agents and appropriate underutilized 2000 Server Machine to be used as relay server.