Security Review #:_____

Field Work Steps

1. **Document all machines**
    a. Complete systems inventory list *
    b. Map network(s) with nmap
2. **Verify firewalls and scan for vulnerabilities**
    a. Firewall rules list (for both hardware and software firewalls) *
    b. Scan high-profile machines with Rapid7
3. **Penetration test**
    a. Use Rapid7 and/or other Commercial Vulnerability Scanners
4. **Network based applications**
    a. Complete departmental networked based application list *
    b. May setup client sessions to any servers and log traffic
        i. Inspect traffic for sensitive information sent in the clear
        ii. Determine potential attack vectors
    c. Web based applications
        i. Use Rapid7
        ii. Check for injection type attacks
        iii. Check web content for policy compliance
    d. Other network based applications
        i. Check application versions reported by scanners
        ii. Attempt to find vulnerabilities in custom software
5. **Local security**
    a. Check for firewalls and antivirus
    b. Use CIS tools to get a baseline score
    c. Scan drives for keywords related to sensitive data (Find_SSNs,Find_CCNs)*
6. **Physical security and data backups**
    a. Site walkthrough
        i. Verify controlled access to any machine or media with sensitive data
        ii. Assess any potential physical vulnerability
    b. Check for daily backup schedule of any critical data
        i. Offsite copies
        ii. All backup media has controlled access
        iii. Verified restore process
        iv. Backup media is degaussed before disposal
7. **Mobile systems (laptops, PDAs)**
    a. Check for special policies and procedures for laptop use
    b. Analyze uses and recommend changes to minimize sensitive data leakage

* These items needed to be completed by the department's technical staff