

Information & Systems/Security Compliance

Information Security Vulnerability Assessment Program



Vulnerability Assessment Program

Description

- Service offered by ISS/C
- Requires high degree of coordination & collaboration
- Uses templates: “Assessment Profiles”
- Review of infrastructure, network, devices
- Report of findings
- Remediation & consultation



Vulnerability Assessment Program

Applicability

- **Current susceptibility to security vulnerabilities**
 - **Preventive measures v. forced remediation (due to exploit)... Which costs less?**
- **Compliance with regulatory requirements**
 - **HIPAA, GLBA, industry practices, etc.**
- **Reduce the risk of public notification or disclosure**
- **Establish case for required or additional resources**



Vulnerability Assessment Program

Activities

- Policies, standards, procedures
- Configuration: Server, network, devices
- Network and PC scans
- Web applications
- Password cracking
- Google hacking
- Spot checks



Vulnerability Assessment Program

Reporting

- **Delivery within 15 business days**
- **Executive summary, Positive findings, Detail**
- **Categories: Critical, High, Medium, Low**
- **Critical findings: reported within 24 hours**
- **Classified as “Legally/Contractually Restricted”**



Vulnerability Assessment Program

Remediation

- **“Critical”**: within 2 business days
- **“High”**: within 5 business days
- **“Medium”**: within 20 business days
- **“Low”**: Optional - within 6 months if fixing it is part of normal upgrade or patching procedure



