COMPLIANCE COMPONENT

DEFINITION	
Name	Security Testing
Description	Security Testing is a methodology in which evaluators attempt to circumvent the security features of a system and identify methods of gaining access by using tools and techniques used by attackers.
Rationale	Security Testing is a critical component of the security plan that allows agencies to improve the security posture of their organization.
Benefits	• Highlights vulnerabilities and allows agencies the opportunity to mitigate them before they are exploited • Aids agencies in making cost-effective decisions to enhance their security posture • Mitigates the loss of production time in applications and systems that could be compromised • Mitigates the compromise of confidential/sensitive information and data loss

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Security
Specify the Discipline Name	Management Controls
Specify the Technology Area Name	Security Risk Management
Specify the Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	• Agencies should conduct Security Testing on an annual basis to ensure that they are in compliance with the Missouri Application Enterprise Architecture (MAEA) and are maintaining the required security posture. • Security Testing has 9 functional areas: 1. Network Scanning 2. Vulnerability Scanning 3. Password Cracking 4. Log Review 5. Integrity Checkers 6. Virus/Malware Detection 7. War Dialing

8. War Driving (802.11 or wireless LAN testing)
9. Penetration Testing

1. Network Scanning

- Network scanning enables an agency to maintain control of its IP address space and ensure that authorized hosts are configured to run only approved network services.
  Agencies should conduct network scanning to:
  - Identify unauthorized hosts,
  - Identify vulnerable services,
  - Identify deviations from authorized services,
  - Prepare for penetration testing,
  - Assist in the configuration of the Intrusion Prevention System (IPS), and collect forensic evidence.

- Only designated individuals should conduct the network scanning.

- Use a port scanner to identify:
  - Open ports that do not have a documented business function,
  - Hosts connected to the network,
  - Network services operating on those hosts, and
  - Services that are running.

- Network scanning results should be documented and identified deficiencies mitigated.

2. Vulnerability Scanning

- Vulnerability scanners identify operating systems and major software applications running on hosts and match them with known exposures. Scanners employ large databases of vulnerabilities to identify flaws associated with commonly used operating systems and applications. These are otherwise known as Security Content Automation Protocols (SCAP) tools.

- Agencies should conduct vulnerability scanning to identify:
  - Known application programming code weaknesses,
  - Out-of-date software versions,
  - The need for patches or system upgrades,
  - Deficiencies in regulatory compliance,
  - Compliance with, or deviations from, the agency's security policy.

- Vulnerability scanning results should be documented and discovered deficiencies mitigated.

3. Password Cracking

- Password cracking programs verify that users are employing sufficiently strong passwords.

- Password crackers should be run to ensure correct password

composition throughout an agency. See the Password Controls Compliance Component of the MAEA.

- Password cracking results should be documented and required changes implemented.

4. Log Review

- While not traditionally considered a testing activity, log review and analysis can provide a picture of system activities that can be compared with the security policy. Audit logs should be used to validate that the system is operating according to policies.

- Log Review should be conducted not only in conjunction with security testing, but continued on a regular basis.

- Log Review results should be documented and required changes implemented.

- Agencies should use Security Information and Event Management (SIEM) tools to provide an overview, analysis and correlation of logs from networks, servers, systems, and applications.

5. Integrity Checking

- File integrity checking is a best practice.

- When used, the following guidelines apply:

    - File integrity checkers compute and store a checksum (or hash) for critical files and establish a database of file checksums. This provides a tool to recognize changes to files, particularly unauthorized changes to files on critical servers.

    - Stored checksums should be recomputed during a security test to test the current value against the stored value to identify file modifications.

    - Integrity checking results should be documented and required changes implemented.

6. Virus/Malware Detection Audit

- Virus/Malware Detection Audits are a complete review of the agency virus/malware detection and elimination policy to ensure compliance with the Virus Policy and Best Practices Compliance Component of the MAEA.
    - NOTE: Any entity with a connection to the agency network shall also be required to comply with the minimum requirements of the MAEA Virus Detection and Elimination Compliance Component.

7. War Dialing

- War Dialing consists of dialing a block of numbers from a Public Switched Telephone Network (PSTN) (e.g. 555-1234 to 555-9999) in an attempt to locate modems within an agency's network.

- When performing a War Dialing assessment:
  - Get approval from upper management,
  - Notify all parties that may be affected, -
  - Schedule outside of regular business hours
  - Ensure all numbers that belong to an agency are tested.

- The results from War Dialing should be used to:
  - Determine current modem status,
  - Inventory devices on your Private Branch Exchange (PBX) accessible by PSTN (e.g. Fax machines, modems, multi-function devices, etc),
  - Identify rogue modems that may have been placed on your network,
  - Locate mis-configured remote access servers, and
  - Locate inadequately secured remote access accounts.

- War Dialing results should be documented and required changes implemented.

8. War Driving (802.11 or wireless LAN testing)

- War Driving is the activity of driving around with a Wi-Fi enabled device, in one's vehicle, in order to find unsecured wireless access points and should include passive wireless scanning.

- Once an access point has been located, then it should be determined if the access point is vulnerable. If access is granted, proceed to Penetration Testing.

- War Driving results should be documented and required changes implemented.

9. Penetration Testing

- A penetration test can be designed to simulate an inside and/or an outside attack on operating systems and software applications.

- Penetration testing can be overt or covert.

- Overt penetration testing involves performing a penetration test with the knowledge and consent of the agency's IT staff. Overt penetration testing is the least expensive and most frequently used.

- Covert penetration testing involves performing a penetration test

	without the knowledge of the agency's IT staff but with full knowledge and permission of the upper management. Covert penetration testing, because of the stealth requirements, requires more time and expense. However, it provides a better indication of everyday security of the agency since system administrators will not be on heightened awareness. • Request formal permission for conducting penetration testing prior to starting. This permission, or rules of engagement, must include: o Specific IP addresses/ranges to be tested, o Any restricted hosts (i.e., hosts, systems, subnets, not to be tested), o A list of acceptable testing techniques (e.g. social engineering, DoS, etc.) and tools (password crackers, network sniffers, etc.), o Times when testing is to be conducted (e.g., during business hours, after business hours, etc.), o Identification of a finite period for testing, o IP addresses of the machines from which penetration testing will be conducted so that administrators can differentiate the legitimate penetration testing attacks from actual malicious attacks, o Points of contact for the penetration testing team, and administrators of the targeted systems and networks, and o Handling of information collected by penetration testing team. • Use of Global Positioning System (GPS) based-mapping may also be included in the permission document. • In external penetration testing, initial attacks focus on commonly used protocols such as FTP, HTTP, Telnet, SSH, or SMTP and POP. Testers: o Are not provided with any real information about the target environment other than targeted IP address/ranges and they must covertly collect information before the attack, o Use port scanners and vulnerability scanners to identify target hosts, and o Attempt to compromise all the identified hosts. • An internal penetration test is similar to an external except testers are granted some level of access to the network at a user level. Testers: o Attempt to gain a greater level of access to the network through privilege escalation, and o Are provided with the information about network resources that a user with their provided privileges would normally have. • Penetration testing consists of four phases: o Planning. The planning phase sets the groundwork.

- Rules are identified.
- Management approval is finalized.
- Testing goals are set.

o Discovery. The discovery phase starts the actual testing.

- Techniques used to gather information on the targeted network are:
  - Network scanning (port scanning),
  - Domain Name System (DNS) interrogation,
  - InterNIC (whois) queries,
  - Search of the target agency's web server(s) for information
  - Packet capture,
  - NetBIOS enumeration (generally only during internal tests),
  - Network Information System ([NIS] generally only during internal tests),
  - Banner grabbing, and
  - Vulnerability analysis

o Exploitation. Vulnerabilities discovered in the vulnerability analysis phase may then be exploited in the attack phase. Caution should be used when attacking production systems to ensure the system is not damaged or that the systems performance is not degraded.

- Most vulnerabilities exploited by penetration testing and malicious attackers fall into the following categories:
  - **Kernel Flaws**—Kernel code is the core of an operating system. Any security flaw that occurs in the kernel puts the entire system in danger.
  - **Buffer Overflows**—A buffer overflow occurs when programs do not adequately check input for appropriate length. When this occurs, malicious code can be introduced into the system and executed with the privileges of the running program.
  - **Symbolic Links**—A symbolic link is a file that points to another file. Often there are programs that will change the permissions granted to a file.
  - **File Descriptor Attacks**—File descriptors are nonnegative integers that the system uses to keep track of files rather than using specific filenames.
  - **Race Conditions**—Race conditions can occur when a program or process has entered into a privileged mode but before the program or process has given up its privileged mode.
  - **File and Directory Permissions**—File and directory permissions control the accesses

	that users and processes have to files and directories. Appropriate permissions are critical to the security of any system. • **Malware**—malware programs can be custom built or include publicly available programs. • **Social Engineering**—Social engineering is the technique of using persuasion and/or deception to gain access to, or information about, information systems. • **Insufficient Input Validation** – Many applications fail to fully validate the input they receive from users. • **Misconfigurations** – Mis-configured security settings, particularly insecure default settings. o Reporting. The reporting phase occurs simultaneously with the other three phases of the penetration test. ▪ At the end of the test a final testing report is developed to describe the identified vulnerabilities, provide a risk rating, and give guidance on the mitigation of the discovered weaknesses. ▪ As soon as they are available, the results should be presented to the agency managers. The results of penetration testing should be taken very seriously and discovered vulnerabilities should be mitigated or accepted. ▪ Reporting includes recommended corrective measures such as: • Mitigating discovered vulnerabilities, • Modifying security policies, • Developing and implementing procedures, and • Conducting security awareness training for personnel.
Document Source Reference #	

Compliance Sources

Name	Technical Guide to Information Security Testing and Assessment SP 800-115, Risk Management Guide for Information Technology Systems SP 800-30, Guide for Assessing the Security Controls in Federal Information Systems 800-53A	*Website*	http://csrc.nist.gov/publications/
Contact Information	inquires@nist.gov		
Name		*Website*	

Contact Information	

KEYWORDS

List Keywords	Penetration, vulnerability, risk, assessment

COMPONENT CLASSIFICATION

Provide the Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*
Sunset Date				

COMPONENT SUB-CLASSIFICATION

Sub-Classification	Date	Additional Sub-Classification Information
☐ *Technology Watch*		
☐ *Variance*		
☐ *Conditional Use*		

Rationale for Component Classification

Document the Rationale for Component Classification	

Migration Strategy

Document the Migration Strategy	

Impact Position Statement

Document the Position Statement on Impact	

CURRENT STATUS

Provide the Current Status	☐ *In Development*	☒ *Under Review*	☐ *Approved*	☐ *Rejected*

AUDIT TRAIL

Creation Date		*Date Approved / Rejected*	05/10/2005
Reason for Rejection			
Last Date Reviewed	4/26/2012	*Last Date Updated*	1/12/2012
Reason for Update	Vitality		