**Security Testing**

Owner: Ho Yeung, Lee

Classification: Secret

FIPS-199 SC administrative information = {(confidentiality, HIGH), (integrity, LOW), (availability, LOW)}

Standard: NIST 800-115, OWASP

1. Introduction

1.1. Purpose

Identifies the purpose of the document as well as the organization being tested, the group conducting the testing (or, if an external entity, the organization engaged to conduct the testing), and the purpose of the security test.

1.2. Scope

Identifies test boundaries in terms of actions and expected outcomes.

1.3. Assumptions and Limitations

Identifies any assumptions made by the organization and the test team. These may relate to any aspect of the test to include the test team, installation of appropriate safeguards for test systems, etc.

1.4. Risks

Inherent risks exist when conducting information security tests—particularly in the case of intrusive tests. This section should identify these risks, as well as mitigation techniques and actions to be employed by the test team to reduce them.

1.5. Document Structure

Outlines the ROE’s structure, and describes the content of each section. 2. Logistics

2.1. Personnel

Identifies by name all personnel assigned to the security testing task, as well as key personnel from the organization being tested. Should include a table with all points of contact for the test team, appropriate management personnel, and the incident response team. If applicable, security clearances or comparable background check details should also be provided.

2.2. Test Schedule

Details the schedule of testing, and includes information such as critical tests and milestones. This section should also address hours during which the testing will take place—for example, it may be prudent to conduct technical testing of an operational site during evening hours rather than during peak business periods.

2.3. Test Site

Identifies the location or locations from which testing is authorized. If testing will occur on the organization’s site, building and equipment access should be discussed. Physical access should cover requirements such as badges, escorts, and security personnel that the testers may encounter. Equipment access should address areas such as level of access (user or administrator) to the systems and/or network, and physical access to computer rooms or specific racks that these rooms contain. Areas to which the test team will not be given access should be identified here as well.

If testing will be conducted from a remote location such as a rented server farm or test lab, details of the test site architecture should be included in this section.

2.4. Test Equipment

Identifies equipment that the test team will use to conduct the information security tests. This section should also identify the method of differentiating between the organization’s systems and the systems conducting the testing—for example, if the test team’s systems are identified by MAC, keeping track of test systems could be handled through use of network discovery software. In addition to hardware, tools authorized for use on the network should be identified. It would also be appropriate to include a write-up of each tool in an appendix.

3. Communication Strategy

3.1. General Communication

Discusses frequency and methods of communication. For example, identify meeting schedule, locations, and conference call information if appropriate.

3.2. Incident Handling and Response

This section is critical in the event that an incident occurs on the network while testing is in progress. Criteria for halting the information security testing should be provided, as should details on the test team’s course of action in the event that a test procedure negatively impacts the network or an adversary attacks the organization while testing is underway. The organization’s incident response call tree/chain of command should be provided in a quick-reference format. A process for reinstating the test team and resuming testing should also be provided.

4. Target System/Network

Identifies the systems and/or networks to be tested throughout the information security testing process. Information should include authorized and unauthorized IP addresses or other distinguishing identifiers, if appropriate, for the systems (servers, workstations, firewalls, routers, etc.), operating systems, and any applications to be tested. It is also crucial to identify any system not authorized for testing—this is referred to as the “exclude list.”

5. Testing Execution

This section is specific to test type and scope, but should detail allowable and unallowable activities and include a description of the information security testing methodology. If necessary, an assessment plan should be developed that complements the ROE—this could be either an appendix or a separate document.

5.1. Nontechnical Test Components

Identifies nontechnical test activities that will take place, and includes information to help identify the types of policies, procedures, and other documents that should be reviewed. If interviews or site surveys are to be conducted, guidelines should be established for advance approval of the interview list and questions. If physical security of information systems is in the scope of the testing, procedures should be determined and a form—with appropriate signatures and contact information—generated for the test team to show to law enforcement or onsite security personnel in the event that they are questioned.

5.2. Technical Test Components

Includes the type of technical testing to be conducted (e.g., network scanning, discovery, penetration testing); discusses whether files are authorized to be installed, created, modified, and/or executed to facilitate testing; and explains the required actions for those files once testing is completed. Any additional information regarding the technical testing of the organization’s systems and networks should also be included in this section. Significant detail should be included on what activities will occur on the target network to ensure that all parties are aware of what is authorized and to be expected as a result of the testing.

5.3. Data Handling

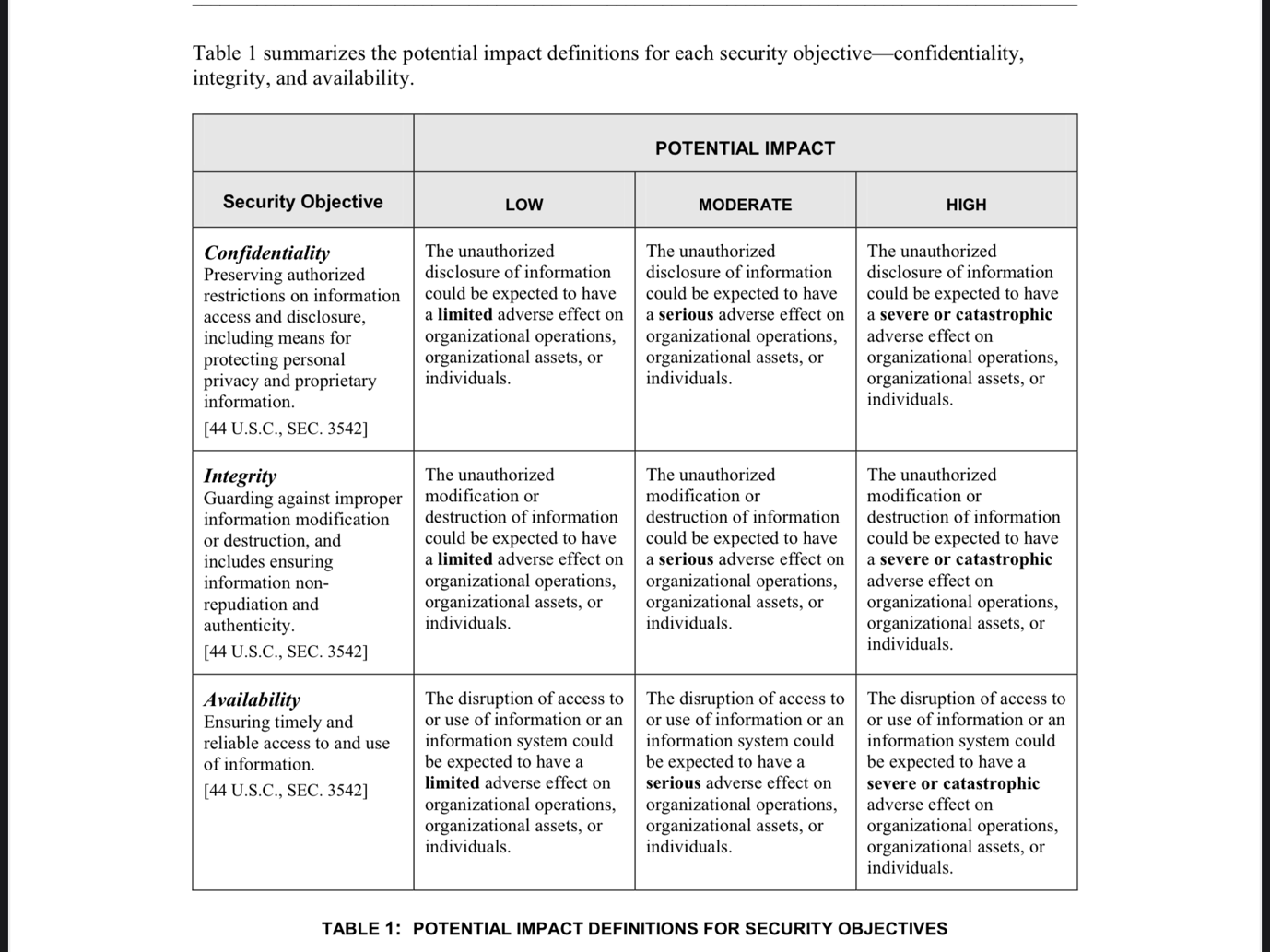
Identifies guidelines for gathering, storing, transmitting, and destroying test data, and establishes detailed, unambiguous requirements for data handling. Keep in mind that data results from any type of information security test will identify vulnerabilities that an adversary can exploit, and should be considered sensitive.

6. Reporting

Details reporting requirements and the report deliverables expected to be provided throughout the testing process and at its conclusion. Minimum information to be provided in each report (e.g., vulnerabilities and recommended mitigation techniques) and the frequency with which the reports will be delivered (e.g., daily status reports) should be included. A template may be provided as an appendix to the ROE to demonstrate report format and content.

7. Signature Page

Designed to identify accountable parties and ensure that they know and understand their responsibilities throughout the testing process. At a minimum, the test team leader and the organization’s senior management (CSO, CISO, CIO, etc.) should sign the ROE stating that they understand the test’s scope and boundaries.

**Appendix**

**FIPS-199**