

Sample Outline of Certification Report

1. Introduction and Summary

Briefly describe the system and summarize the evaluation findings and recommendations.

2. Background

Provide contextual information for the Designated Approving Authority (DAA). It is important to include the security standards or policies applied to the system. Another important item is a list of the general functional characteristics of the system that generically influence its certifiability (e.g., the presence or absence of user programming). Also include the system boundaries and security assumptions about areas outside the boundaries.

3. Major Findings

3.1 General Control Posture.

Summarize the controls that are in place and their general roles in protecting assets against threats and preventing exposures. This information is important to maintain perspective, and emphasizes those areas where safeguards are acceptable.

3.2 Vulnerabilities

Summarize major vulnerabilities. Vulnerabilities described here are divided into two categories: proposed residual vulnerabilities and proposed vulnerabilities requiring correction. This format serves as both a summary of findings and a recommendation of which vulnerabilities to accept and which to correct.

4. Recommended Corrective Actions

Recommend and prioritize corrective actions. Include anticipated costs and impacts of the corrective actions and who is responsible for completing them. Establish criteria for evaluating the corrections. This section must be complete enough to give the DAA a clear understanding of the implications of either accepting or correcting the vulnerabilities.

5. Certification Process

Summarize the work performed in the certification process. The purpose of this section is to enable the DAA to determine the level of confidence that can be placed in the certification findings. May be useful to include the Certification Plan as an attachment.

Attachment A Proposed Accreditation Statement

This is a critical part of the certification report. This statement summarizes recommended actions and is prepared for the DAA's signature. Judgments and recommendations embodied in the statement are subject to the DAA's approval.

Attachment B (etc.) Detailed Evaluation Report(s)

These reports describe the full set of findings, not just the major ones. The reports should match the way the evaluation work was divided (e.g., application software control, change control, physical security, personnel security, etc.). The reports should follow a standard format.