SYSTEM NAME
CERTIFICATION AND ACCREDITATION STATEMENT

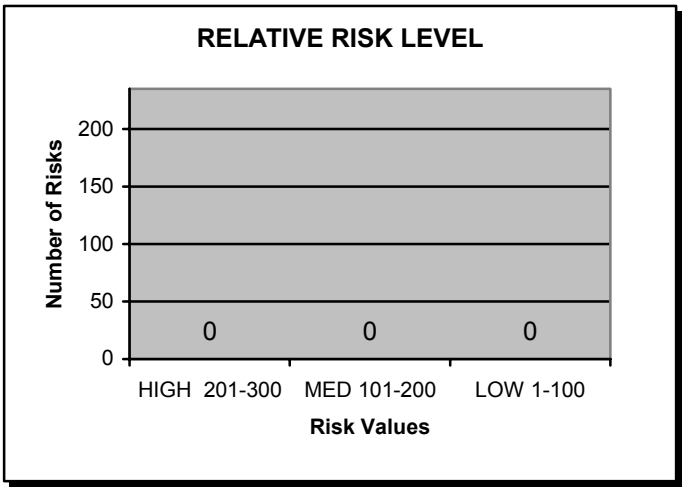
Background

Between start date and end date, a security test and evaluation (ST&E) was conducted on the System Name operated by the organization/office located at location. The ST&E was performed by an independent assessment team under the direction of the undersigned Certifying Agent under the authority of authorizing official, Office, Department of Housing and Urban Development and was conducted in accordance with Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources* and Department of Housing and Urban Development policy and guidance on accreditation. The purpose of the ST&E was to demonstrate, through selected verification techniques and verification procedures documented in the System Name *ST&E Plan* (dated date) and *ST&E Report* (dated date), that necessary security controls that are identified in the System Name *Security Plan* (dated date) are implemented correctly, meet minimum security requirements, are effective in their application, and that the controls adequately mitigate risks described in the System Name *Risk Assessment Report* (dated date). The certification effort provides the Designated Approving Authority with important information necessary to make an informed, risk-based decision regarding the operation of System Name.

Summary of Findings

The results of the certification effort are summarized in the following two figures:

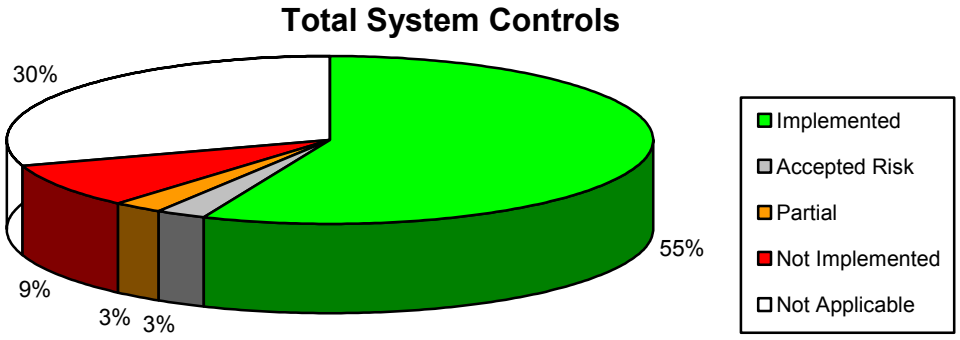
Figure 1



Number vulnerabilities found in System Name controls are ranked as low, medium or high risk. Therefore, System Name is categorized as having a **low**, **medium** or **high** level of risk.

The results of the risk assessment of System Name indicated that the primary risks to system resources related to unlawful/unauthorized acts committed by hackers, computer criminals, and insiders related to system intrusion, fraud, and spoofing. Unintentional user errors and omissions are additional critical risks to system data and operations.

Figure 2



System name management has fully implemented number of 235 of the required IT security controls (percent). Another number (#) controls (percent) have been partially implemented or are in the process of being implemented. Number (#) controls (percent) are not applicable to the system. Residual risk is being accepted for number (#) of the controls (percent). Number controls have not been implemented at this time.

Statement of Compliance

Based on the state of security controls tested and evaluated during the ST&E at Low or Moderate or High Security Certification Level, it is the judgment of the Certifying Agent that, with the exception of corrective actions specified in the attached Plan of Action and Milestones, System Name complies with the general requirements of OMB Circular A-130, Appendix III and with minimum security requirements defined for a Low or Moderate or High sensitivity system by the Department of Housing and Urban Development in accordance with Federal Information Processing Standard 199 and National Institute of Standards and Technology (NIST) Special Publication 800-53. The most significant areas of non-compliance identified are:

- First significant weakness from the POA&M
- Second significant weakness from the POA&M
- etc….

Recommendations

The security controls listed in the System Name security plan have been tested and evaluated by an organization name certification team using the verification techniques and the procedures described in the attached ST&E Results Report to determine if those controls meet minimum security requirements and are effective in their application. Testing has reasonably demonstrated that System Name provides necessary assurance for secure processing. Based on the results of ST&E activities, the undersigned Certifying Agent recommends that the System Owner take action to correct identified vulnerabilities according to the schedule documented in the System Name Plan of Action and Milestones (POA&M), which describes the corrective measures that are necessary to reduce or eliminate the stated vulnerabilities in system controls. I further recommend that the system be authorized for operation by the Designated Approving Authority (DAA), and that identified residual risks be accepted.

_____ _____

Name Date
Certifying Agent
Organization

Certification Statement

Based on my review of documentation contained in the accompanying certification package, I concur with the findings and recommendations of the Certifying Agent. I certify that System Name security controls have been tested at the Low or Moderate or High Security Certification Level, which is commensurate with the sensitivity level of the system and as of this date System Name meets applicable federal security requirements as it operates in its current environment with the exception of vulnerabilities identified in the attached System Name POA&M. I recommend that the Designated Approving Authority accept identified residual risks and authorize System Name processing in its current operational environment by accrediting the system under the provision that all risks be mitigated in accordance with the System Name POA&M. I will ensure that a review of security controls protecting the system is conducted upon any major changes to the current operating environment.

_____ _____

Name, Organization ISSO Date
Certifying Official
Organization

Accreditation Statement

In accordance with the provisions of the HUD Certification and Accreditation Program, after reviewing the security controls that have been implemented and planned, and weighing the remaining residual risks against operational requirements, I authorize operation of System Name

for continued operation under the provision that necessary corrective action is taken to address the following weaknesses.

- Weakness
- …etc.

This authorization is my formal declaration that the majority of security controls for the System Name have been properly implemented and are functioning correctly; however, additional security controls are needed to ensure that a satisfactory level of security has been achieved. System name may be operated in a restricted mode until all high and medium risks identified in the Plan of Action and Milestones (PO&AM) for the system can be implemented. These restrictions include:

- Restriction on operations (e.g., more frequent review of audit trails)
- …etc.

This authorization is for the existing operating environment of System Name, is contingent upon continued application of the security controls in place, and is valid for a period of three (3) years from the date of this statement unless a significant change to the IT system requires earlier accreditation. I authorize System Name to operate with residual risks related to the following NIST Special Publication 800-53 requirements:

- Residual risk
- …etc.

I will ensure that the owner of System Name analyzes any significant change in the system's configuration (i.e., hardware, software, and/or firmware) or the system's operating environment to determine its impact on system security, and that the system owner takes appropriate action to maintain a level of security consistent with the requirements for this action.

The organization Information System Security Officer (ISSO) will retain a copy of this accreditation letter with all supporting documentation as a permanent record.

_____ _____

Name Date
Designated Approving Authority
Organization

cc: Name, Chief Information Security Officer

Attachments:
1. System Security Plan
2. Risk Assessment
3. Security Test and Evaluation Plan and Results
4. Plan of Action and Milestones

5. Minimum Security Baseline Assessment