DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

CERTIFICATION AND ACCREDITATION PROCESS GUIDE

Version 1.0

Document Configuration Control

Version	Release Date	Summary of Changes

TABLE OF CONTENTS

Section 1.0 Introduction

The Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Information Resources* requires agencies to perform a review of the security controls within each information system and formally approve the system's operation. The formal approval by a senior agency official, or authorization for processing, is commonly known as accreditation. The technical and non-technical evaluation of a system that allows the senior official to make a risk-based decision to accredit the system is commonly known as certification. The National Institute for Standards and Technology (NIST) Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, establishes standards for certifying and accrediting Federal information systems. NIST 800-37 provides guidance on certification and accreditation processes and activities, general tasks, and roles and responsibilities for certifying and accrediting systems to provide information assurance of a system or facility. Processes described in NIST SP 800-37 can be used to certify and accredit any information system in any stage of the system's life cycle.

Purpose

In order to meet the intent of OMB Circular A-130, Appendix III, the Department of Housing and Urban Development (HUD) has adopted NIST SP 800-37 guidelines to form the HUD Certification and Accreditation Process (CAP). This *HUD Certification and Accreditation Process Guide* provides an overview of the HUD CAP and is designed to guide HUD organizational elements and certifying agents/teams within HUD through the certification and accreditation (C&A) process. HUD CAP enables the certification of information systems against documented system-specific security requirements, permits the designated approving authority to make risk-based decisions regarding the secure operation of the system, and allows maintenance of the accredited security posture throughout the system's life cycle.

Scope

The guidance contained in this document is applicable to all organizations within HUD, and specifically to any certifying agents/teams conducting C&A activities for HUD, to include C&A staff members or contractors. The document will be used to guide C&A activities related to the certification and accreditation of non-national security systems only.

Document Overview

Section 1.0, the Introduction, documents the purpose and scope of this document.

Section 2.0 defines the roles in the HUD CAP.

Section 3.0 provides an overview of HUD CAP phases and tasks.

Section 4.0 describes Security Certification Levels of effort.

Section 5.0 identifies supporting documentation required for the HUD CAP, and identifies templates that can be used to meet CAP requirements.

Section 6.0 defines the terms that are related to C&A

Section 2.0 Roles in the HUD CAP

There are three essential roles in the HUD Certification and Accreditation Process (CAP). At a minimum, a system owner, Designated Approving Authority (DAA), and certifying agent are required to implement the process. Additional roles are included in the CAP to enhance efficiency of the process, and to increase the integrity, reliability, and objectivity of C&A decisions. Primary and secondary C&A roles are identified in the following paragraphs.

System Owner - The system owner is the HUD official responsible for the overall development, procurement, integration, operation and maintenance of a HUD information system. The system owner coordinates security of information processed by the system throughout its life cycle, from design through implementation and maintenance. The system owner is responsible for preparing and maintaining the system security plan and ensures the system is deployed and operated according to security requirements documented in the plan. The system owner is also responsible for deciding who has access to the system (and with what types of privileges or access rights) and ensures that system users and support personnel receive necessary security training (e.g., instruction in rules of behavior). The system owner notifies the DAS ISSO when there is a need to certify and accredit the information system, ensures that appropriate resources are available for the effort, and provides the necessary system-related documentation and support to the Certifying Agent. The system owner reviews security assessment results received from the Certifying Agent, and after taking appropriate steps to reduce or eliminate vulnerabilities, the system owner assembles the security accreditation package and submits the package to the authorizing official for adjudication.

Designated Approving Authority - The designated approving authority (DAA) is a senior HUD management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to HUD operations, assets, or individuals. Through security accreditation, the DAA assumes responsibility and is accountable for the risks associated with operating an information system. The DAA will normally have the authority to oversee the budget and business operations of the information system and is often called upon to approve system security requirements, system security plans, and memoranda of agreement/understanding. In addition to authorizing operation of an information system, the authorizing official can deny authorization to operate the system (or if the system is already operational, to halt operations) if unacceptable security risks exist. With the increasing complexities of agency missions and organizations, it is possible that a particular information system may involve multiple DAAs. If so, agreements will be established among the DAAs and will be documented in the system security plan. In such cases, a lead authorizing official will be agreed upon to represent the interests of the other approving authorities. The DAA has inherent U.S. government authority and, as such, must be a government employee. To assure segregation of duties the role of DAA and system owner will not be performed by the same individual.

Certifying Agent - The certifying agent is an individual, group, or organization responsible for conducting a security certification, or comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The certifying agent also recommends corrective actions to reduce or eliminate vulnerabilities in system security controls. The certifying aAgent provides an independent assessment of the system security plan to ensure the plan identifies security controls for the system that adequately meet all applicable security requirements. Once the certification effort is complete, the certifying authority reports to the DAA whether the system should be accredited on the basis of the existing risk.

User Representative - The user representative assists in the security certification and accreditation process, when needed, to ensure mission requirements are satisfied while meeting the security requirements and employing the security controls defined in the system security plan. User representatives are individuals that represent the operational interests of the user community and serve as liaisons for that community throughout the system development life cycle of the information system.

Chief Information Officer - The Chief Information Officer (CIO) is the HUD official responsible for: designating a senior HUD information security officer; developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements; training and overseeing personnel with significant responsibilities for information security; assisting senior HUD officials concerning their security responsibilities; and in coordination with other senior HUD officials, reporting annually to the Secretary of Transportation on the effectiveness of the HUD information security program, including progress of remedial actions. The CIO, with the support of the senior HUD information security officer, works closely with DAAs to ensure that an agency-wide security program is effectively implemented, that the certifications and accreditations required across the department are accomplished in a timely and cost-effective manner, and that there is centralized reporting of all security-related activities. To achieve a high degree of cost effectiveness with regard to security, the CIO encourages the maximum reuse and sharing of security-related information including: threat and vulnerability assessments; risk assessments; results from common security control assessments; and any other general information that may be of assistance to information system owners and their supporting security staffs. In addition to the above duties, the CIO and DAAs determine the appropriate allocation of resources dedicated to the protection of HUD information systems based on organizational priorities. In certain instances, the CIO may be designated as the DAA for department-wide general support systems or as a co-DAA with other authorizing officials for selected HUD information systems.

Senior HUD Information Security Officer - The Chief Information Security Officer (CISO) is designated as the Department's senior information security officer, and as such is the HUD official responsible for carrying out the CIO's responsibilities under FISMA; possessing the professional qualifications, including training and experience, required to administer the information security program functions; having information security duties as that official's primary duty; and heading an office with the mission and resources to assist in ensuring agency compliance with FISMA. The CISO serves as HUD's program manager for certification and accreditation, and is the HUD official responsible for ensuring that HUD information systems are certified and accredited prior to being placed into production, and serves as the CIO's primary liaison to managers of major HUD organizations and DAAs.

Deputy Assistant Secretary (DAS) ISSO - The information system security officer (ISSO) for each office of the Deputy Assistant Secretary is the individual responsible to the DAA or the Deputy Assistant Secretary for ensuring that appropriate operational security posture is maintained for information systems belonging to the organization. Each DAS level ISSO also serves as the principal advisor to senior DAS management, DAAs, and system owners on all matters (technical and otherwise) involving the security of information systems. The DAS ISSO may be called upon to assist in the development of the system security policy and to ensure compliance with that policy on a routine basis.

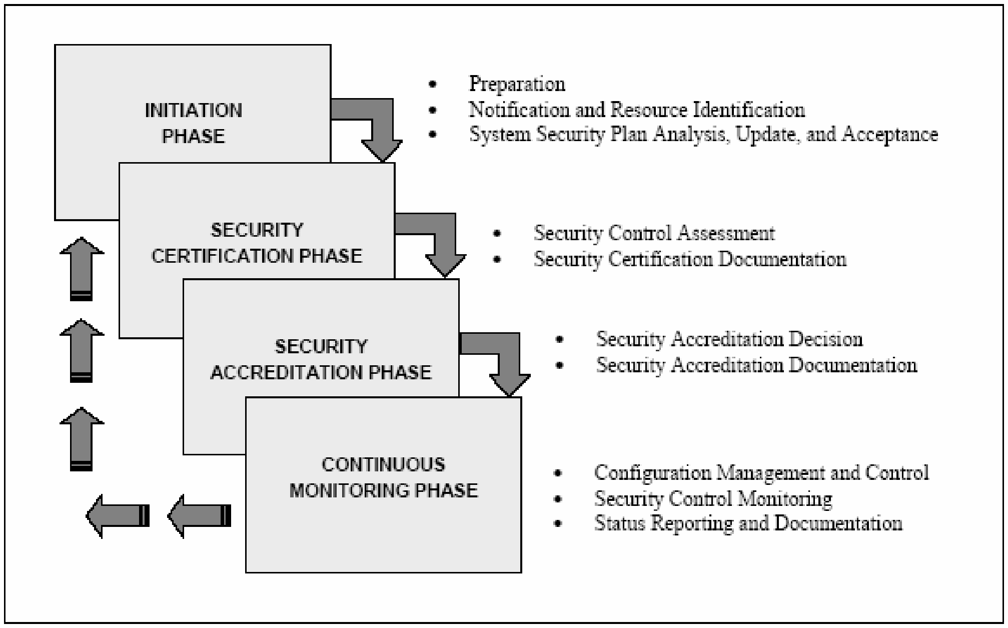
Information System Security Officer (ISSO) - The information system security officer (ISSO) is the individual responsible to the information system owner for ensuring the appropriate operational security posture is maintained for an information system. The information system security officer also serves as the principal advisor to the information system owner on all matters (technical and otherwise) involving the security of the information system. The information system security officer typically has the detailed knowledge and expertise required to manage the security aspects of the information system and, in many agencies, is assigned responsibility for the day-to-day security operations of the system. This responsibility may also include, but is not limited to, physical security, personnel security, incident handling, and security training and awareness. In close coordination with the information system owner, the information system security officer often plays an active role in developing and updating the system security plan as well as in managing and controlling changes to the system and assessing the security impact of those changes.

Information Owner - The system owner is a HUD official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. The system owner is responsible for establishing rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with other organizations. The owner of the information stored within, processed by, or transmitted by an information system is not necessarily the information system owner. Also, a single information system may utilize information from multiple system owners. Information owners should provide input to information system owners regarding security requirements and security controls for the systems processing, storing or transmitting the information.

Section 3.0 Certification and Accreditation Phases and Tasks

The HUD security certification and accreditation process (CAP) consists of four distinct phases: Initiation, Security Certification, Security Accreditation, and Continuous Monitoring. Each phase consists of a set of defined tasks and subtasks that are to be performed by responsible individuals (e.g., the CIO, DAA, DAS ISSO, system owner, system owner, ISSO, Certifying Agent, and User Representative). Security certification and accreditation activities can be applied to an information system at appropriate phases in the system development life cycle. Additionally, the activities can be tailored to apply a level of effort and rigor that is most suitable for the system undergoing security certification and accreditation. The following figure provides a high-level view of the HUD security certification and accreditation process including the tasks associated with each phase in the process.

Figure 1: The HUD C&A Process (CAP)


INITIATION PHASE
• Preparation
• Notification and Resource Identification
• System Security Plan Analysis, Update, and Acceptance
SECURITY CERTIFICATION PHASE
• Security Control Assessment
• Security Certification Documentation
SECURITY ACCREDITATION PHASE
• Security Accreditation Decision
• Security Accreditation Documentation
CONTINUOUS MONITORING PHASE
• Configuration Management and Control
• Security Control Monitoring
• Status Reporting and Documentation

Phase 1 - Initiation

The Initiation Phase consists of three tasks: preparation, notification and resource identification, and system security plan analysis, update, and acceptance. The purpose of this phase is to ensure that the system owner and the DAS ISSO are in agreement with the contents of the system security plan, including the system's documented security requirements, before the Certifying Agent begins the assessment of the security controls in the information system. A significant portion of the information needed for this phase should have been previously developed by the system owner. For new information systems or systems undergoing major upgrades, this information is normally produced during the initiation phase of the system development life cycle when system requirements are established. For legacy systems currently in the operations and maintenance phase of the system development life cycle, this information is obtained from the most recent security plan and risk assessment. The Initiation Phase serves as a checkpoint to confirm that the system security plan and risk assessment have been completed. If a system owner has not completed a risk assessment and a system security plan, those activities should be completed prior to proceeding with the security certification and accreditation process. Tasks and sub-tasks related to this phase are identified in Table 1 below.

Table 1: Initiation Phase Tasks

Task/ Sub-Task	Task Title	Description	Responsibility
1.0	**Preparation**		
1.1	System Description	Confirm that the system has been fully described and documented in the system security plan or an equivalent document.	System Owner
1.2	Security Categorization	Confirm that the security category of the information system has been determined and documented in the system security plan or an equivalent document.	System Owner
1.3	Threat Identification	Confirm that potential threats that could exploit information system flaws or weaknesses have been identified and documented in the system security plan, risk assessment, or an equivalent document.	System Owner
1.4	Vulnerability Identification	Confirm that flaws or weaknesses in the information system that could be exploited by potential threat sources have been identified and documented in the system security plan, risk assessment, or an equivalent document.	System Owner
1.5	Security Control Identification	Confirm that the security controls (either planned or implemented) for the information system have been identified and documented in the system security plan or an equivalent document.	System Owner
1.6	Initial Risk Determination	Confirm that the risk to agency operations, agency assets, or individuals has been determined and documented in the system security plan, risk assessment, or an equivalent document.	System Owner
2.0	**Notification and Resource Identification**		
2.1	Notification	Inform the DAS ISSO, DAA, Certifying Agent, User Representatives, and other interested HUD officials that the information system requires security certification and accreditation support.	System Owner
2.2	Planning and Resources	Determine the level of effort and resources required for the security certification and accreditation of the information system (including organizations involved) and prepare a project plan.	DAA; DAS ISSO; System Owner; Certifying Agent
3.0	**System Security Plan Analysis, Update, And Acceptance**		
3.1	Security Categorization Review	Review the FIPS 199 security categorization described in the security plan to determine if the assigned impact values are consistent with HUD's actual mission requirements with respect to the potential loss of confidentiality, integrity, and availability.	DAA; DAS ISSO; System Owner; Certifying Agent
3.2	System Security Plan Analysis	Analyze the security plan to determine if the vulnerabilities in the system and the resulting risk to HUD operations, assets, or individuals is actually what the plan would produce, if implemented.	DAA; DAS ISSO; System Owner; Certifying Agent

Task/ Sub-Task	Task Title	Description	Responsibility
3.3	System Security Plan Update	Update the security plan based on the results of the independent analysis and recommendations of the Certifying Agent, DAA, and DAS ISSO.	System Owner
3.4	System Security Plan Acceptance	Review the security plan to determine if the risk to HUD operations, assets, or individuals is acceptable.	DAA; DAS ISSO

Phase 2 – Security Certification

The Security Certification Phase consists of two tasks: security control assessment; and security certification documentation. The purpose of the this phase is to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This phase also addresses specific actions taken or planned to correct deficiencies in the security controls and to reduce or eliminate known vulnerabilities in the information system. Upon successful completion of this phase, the DAA will have the information necessary to determine the risk to HUD operations, assets, or individuals, and accordingly will be able to render an appropriate accreditation decision regarding the security of the system. Tasks and sub-tasks related to this phase are identified in Table 2 below.

Table 2: Security Certification Phase Tasks

Task/ Sub-Task	Task Title	Description	Responsibility
4.0	**Security Control Assessment**		
4.1	Documentation and Supporting Materials Collection	Assemble documentation and supporting materials necessary for the assessment of system security controls; if these documents include previous assessments of security controls, review the findings, results, and evidence.	System owner; Certifying Agent
4.2	Methods and Procedures Identification	Select, or develop when needed, appropriate methods and procedures to assess the management, operational, and technical security controls in the system.	Certifying Agent
4.3	Security Assessment	Assess the management, operational and technical security controls in the system using methods and procedures selected or developed.	Certifying Agent
4.4	Security Assessment Report Preparation	Prepare the final security assessment report.	Certifying Agent
5.0	**Security Certification Documentation**		
5.1	Findings and Recommendations Submission	Provide the system owner with the security assessment report.	Certifying Agent
5.2	System Security Plan Update	Update the security plan (and risk assessment) based on the results of the security assessment with any modifications to system security controls.	System Owner
5.3	POA&M	Prepare the plan of action and milestones	System Owner

Task/ Sub-Task	Task Title	Description	Responsibility
	Preparation	(POA&M) based on the results of the security assessment.	
5.4	Accreditation Package Assembly	Assemble the final security accreditation package and submit to the DAA.	System Owner

To ensure that security certification tasks are performed in an impartial and unbiased manner, the Certifying Agent should be in a position that is independent from the persons directly responsible for the development of the information system and from the day-to-day operation of the system. The Certifying Agent should also be independent of those individuals responsible for correcting security deficiencies identified during the security certification. The independence of the Certifying Agent is an important factor in assessing the credibility of the security assessment results and ensuring the authorizing official receives the most objective information possible in order to make an informed, risk-based, accreditation decision. However, when the potential impact on agency operations, agency assets, or individuals is low (i.e. low confidentiality, integrity, and availability impacts), there is no requirement for an independent Certifying Agent and a self-assessment is reasonable and appropriate.

Phase 3 – Security Accreditation

The Security Accreditation Phase consists of two tasks: (i) security accreditation decision; and (ii) security accreditation documentation. The purpose of this phase is to determine if the remaining known vulnerabilities in the information system (after the implementation of an agreed-upon set of security controls) pose an acceptable level of risk to HUD operations, assets, or personnel. Upon successful completion of this phase, the system owner will have either authorization to operate the system or the DAA's denial of authorization to operate the system. Tasks and sub-tasks related to this phase are identified in Table 3 below.

Table 3: Security Accreditation Phase Tasks

Task/ Sub-Task	Task Title	Description	Responsibility
6.0	**Security Accreditation Decision**		
6.1	Final Risk Determination	Determine the risk to HUD operations, assets, or individuals based on the vulnerabilities in the system and any planned or completed corrective actions to reduce or eliminate those vulnerabilities.	DAA
6.2	Risk Acceptance Determination	Determine if the risk to HUD operations, assets, or individuals is acceptable and prepare the final security accreditation decision letter.	DAA
7.0	**Security Accreditation Documentation**		
7.1	Security Accreditation Package Transmission	Provide copies of the final security accreditation package including the accreditation decision letter (in either paper or electronic form), to the system owner and any other HUD officials having an interest in the security of the system.	DAA
7.2	System Security Plan Update	Update the security plan based on the final determination of risk to HUD operations, assets, or individuals.	System Owner

Phase 4 – Continuous Monitoring

The Continuous Monitoring Phase consists of three tasks: configuration management and control, security control monitoring, and status reporting and documentation. The purpose of this phase is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the authorizing official when changes occur that may impact on the security of the system. The Continuous Monitoring Phase begins after the system has been certified and accredited for operations, and the activities in this phase are performed continuously throughout the life cycle of the information system. Tasks and sub-tasks related to this phase are identified in Table 4 below.

Table 4: Continuous Monitoring Phase Tasks

Task/ Sub-Task	Task Title	Description	Responsibility
8.0	**Configuration Management and Control**		
8.1	Documentation of System Changes	Using established agency configuration management and control procedures, document proposed or actual changes to the system (including hardware, software, firmware, and surrounding environment).	System Owner
8.2	Security Impact Analysis	Analyze proposed or actual changes to the system (including hardware, software, firmware, and surrounding environment) to determine the security impact of such changes.	System Owner
9.0	**Security Control Monitoring**		
9.1	Security Control Selection	Select the security controls in the system to be monitored on a continuous basis.	System Owner
9.2	Selected Security Control Assessment	Assess an agreed-upon set of security controls in the system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	System Owner
10.0	**Status Reporting and Documentation**		
10.1	System Security Plan Update	Update the security plan based on the documented changes to the system (including hardware, software, firmware, and surrounding environment) and the results of the continuous monitoring process.	System Owner
10.2	POA&M Update	Update the plan of action and milestones based on the documented changes to the system (including hardware, software, firmware, and surrounding environment) and the results of the continuous monitoring process.	System Owner
10.3	Status Reporting	Report the security status of the information system to the DAA and DAS ISSO.	System Owner

An orderly and disciplined approach to managing, controlling, and documenting changes to an information system is critical to the continuous assessment of the security controls that protect the system. It is important to record any relevant information about the specific proposed or actual changes to the hardware, firmware, or software such as version or release numbers, descriptions of new or modified features or capabilities, and security implementation guidance. Any changes to the information system environment should also be recorded to include modifications to the physical plant; expansion or contraction of the user community; addition of new interconnections with other systems; changes in laws, directives, policies, and regulations; and/or changes in sensitivity of information processed. The system owner and ISSO should use this information in assessing the potential security impact of the proposed or actual changes to the information system. **Significant changes to the information system should not be undertaken prior to assessing the security impact of such changes**.

Section 4.0 Security Certification Levels

The fundamental purpose of the certification process is to determine if the security controls for the IT system are correctly implemented and are effective in their application. Certification levels described in this section establish the level of effort and test methods to be used to verify security controls for security test and evaluation efforts.

There is a general expectation that the level of effort for security certification and accreditation (expressed in terms of degree of rigor and formality) should be scalable to the security sensitivity and criticality of the information system. That is, HUD information systems with greater sensitivity and/or criticality have greater potential for adversely affecting HUD operations, assets, or personnel and therefore demand greater scrutiny with regard to the assessment of those security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The level of effort applied to the security certification and accreditation tasks and subtasks should be commensurate with the rigor and formality of the assessment methods and procedures selected. The controls specified in NIST Special Publication 800-53 will be applied as the framework for identification of minimum controls necessary for the security of all HUD information systems.

The correct and effective implementation of these controls provides assurance that system security requirements have been satisfied. There are many verification techniques that can be employed during the C&A process to determine the correctness and effectiveness of the security controls. These techniques include:

- Interviewing HUD employee and contractor personnel associated with the security of the system;
- Reviewing and examining security-related policies, procedures, and documentation;
- Observing security-related activities and operations;
- Analyzing, testing, and evaluating the security relevant and security critical aspects of system hardware, software, firmware, and operations; and
- Conducting demonstrations and exercises.

There are three certification levels defined in the HUD C&A Process: Low Security Certification Level, Moderate Security Certification Level, and High Security Certification Level. Each of the successive certification levels provides additional rigor and intensity in the application of the verification techniques to determine compliance with the security requirements and to demonstrate the correctness and effectiveness of the security controls. The security certification levels are based on the "high water mark" of the IT system's sensitivity, based on the system's confidentiality, integrity and availability levels according to FIPS 199, and can be adjusted based on the IT system's criticality.[1] NIST SP 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems* when available will provide instructions on verification techniques for controls of systems at each certification level.

[1] An IT system's sensitivity and criticality can be determined using the *HUD IT System Inventory Guide*.

Low Security Certification Level (SCL)

Low SCL is the *entry-level* certification for an IT system. This certification level is appropriate for systems with low levels of concern for system sensitivity, where considerations for confidentiality, integrity, and availability are each rated "low" as outlined in the HUD *IT System Certification and Accreditation Inventory Guide*. Low SCL certifications do not require independent assessments and are normally performed by the system owner or a member of the system owner's staff using self-assessment questionnaires or specialized checklists.[2] These assessments are intended to demonstrate at relatively low levels of assurance that the security controls for the system are correctly implemented and are effective in their application. Low SCL certifications are relatively low intensity endeavors that can be accomplished with minimal resources using simple verification techniques such as personnel interviews, documentation reviews, and observations. Additionally, a detailed contingency plan is not normally required for a Low SCL certification where an IT system would be assigned low criticality and low availability requirements.

Moderate Security Certification Level

Moderate SCL is the *mid-level* certification for IT systems. This certification level is appropriate for systems with a moderate level of concern for confidentiality, integrity, and/or availability as outlined in the HUD *IT System Certification and Accreditation Inventory Guide*. Moderate SCL certifications involve the assessment of information systems by independent Certifying Agents building on the verification techniques and procedures from Low SCL and adding more substantial techniques and procedures, as appropriate. These independent assessments are intended to demonstrate at moderate levels of assurance that the security controls are correctly implemented and are effective in their application. Moderate SCL certifications are moderate intensity endeavors that can be accomplished with limited to moderate resources using standard, commercially available, assessment tools and verification techniques such as personnel interviews, documentation reviews, observations, demonstrations, and limited ST&E activities, (e.g., limited functional testing, regression analysis and testing, and optional penetration testing). The contingency plan must be developed commensurate with the IT system's criticality and availability requirements where a detailed contingency plan might not be required.

High Security Certification Level

High SCL is the *top-level* certification for IT systems. This certification level is appropriate for systems with a high level of concern for confidentiality, integrity, and/or availability as outlined in the HUD *IT System Certification and Accreditation Inventory Guide.* High SCL certifications call for an independent assessment of the system building on the verification techniques and procedures from Low SCL and Moderate SCL certifications and employing the most rigorous verification techniques, as appropriate. These independent assessments are intended to demonstrate at high levels of assurance that the security controls for IT systems are correctly implemented and are effective in their application. High SCL certifications are high intensity endeavors that can be accomplished with substantial resources using the most advanced assessment tools and verification techniques available, (i.e., system design analysis, extended functional testing with test coverage analysis, regression analysis/testing, demonstrations, exercises, and penetration testing with Red Team option).

[2] HUD's minimum security requirements is based on NIST 800-53, and can be found in the Minimum Security Baseline Assessment.

Certification Level Selection

After the particular levels of concern for confidentiality, integrity, and availability have been determined in accordance with FIPS 199 and the HUD *IT System Certification and Accreditation Inventory Guide* and are documented in the system security plan, the initial certification level can be selected. If any level of concern for confidentiality, integrity, or availability is high, then High SCL is selected. If there are no high levels of concern, and if any level of concern for confidentiality, integrity and availability is moderate, then Moderate SCL is selected. If all levels of concern for confidentiality, integrity, and availability are low, then Low SCL is selected.

Section 5.0 CAP Supporting Documentation

The HUD Certification and Accreditation Process (CAP) verifies the correctness and effectiveness of security controls employed in an information system as well as ensures adequate security is maintained. OMB Circular A-130, Appendix III, requires federal agencies plan for security and dictates that certain security controls must be in place for a general support system or a major application. The CAP guides system owners in ensuring that OMB Circular A-130 controls are properly documented.

The security *accreditation package* documents the results of the security certification and provides the authorizing official with the essential information needed to make a credible, risk-based decision on whether to authorize operation of the information system. Unless specifically designated otherwise, the system owner is responsible for the assembly, compilation, and submission of the security accreditation package. The system owner receives inputs from the ISSO, Certifying Agent, and DAS ISSO during the preparation of the security accreditation package. The accreditation package normally consists of the following documentation:

- The *system security plan*, prepared by the system owner and approved by the DAA and DAS ISSO, provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents for the information system such as the privacy impact assessment, incident response plan, configuration management plan, security configuration checklists, rules of behavior, and any system interconnection agreements. *System security plans* will be developed in accordance with NIST SP 800-18.

- A *technical architecture document* is prepared as a supplement to the system security plan for SCL-3 systems to provide more detail on the system description, its environment, and interconnectivity.

- A *minimum security baseline assessment* will be prepared by the system owner to identify vulnerabilities against a minimum set of security standards. System owners will use NIST SP 800-53 to assess security controls for all HUD information systems.

- The *risk assessment* prepared by the system owner and approved by the DAA and DAS ISSO, documents risks to the information systems by identifying system assets, evaluating threats to these assets, and vulnerabilities to safeguards protecting system assets. The *risk assessment* evaluates the effectiveness and applicability of the minimum security baseline control set and recommends adjustments to minimum safeguards according to system-specific risks. The *risk assessment* will follow a standard methodology approved by NIST (see NIST SP 800-30).

- The *contingency plan* documents management policy and procedures that are designed to maintain or restore business operations supported by the system, potentially at an alternate location, in the event of emergencies, system failures, or disaster. The availability of all HUD information systems having moderate or high availability requirements will be protected through the development of a contingency plan. However, a contingency plan is not required when the availability of system resources is covered by a contingency plan for another system (i.e., general support system). Contingency plans will be developed in accordance with the standard methodology approved by NIST (see NIST SP 800-34).

- The *security test and evaluation (ST&E) plan and results report*, prepared by the Certifying Agent and approved by the system owner and DAA, documents the plan for certifying the system and provides the results of the assessment of security controls in the system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome. The ST&E plan is submitted and approved prior to the beginning of certification testing.

- *HUD-approved IT security baseline configurations* will be used by Certifying Agents as part of certification testing to evaluate platform-specific controls protecting system assets. These IT security baseline configurations will be based on industry standard best practices available and approved by the HUD CISO. The results of testing using these baseline configurations are normally included in the *security test and evaluation (ST&E) plan and results report.*

- A *plan of action and milestones* (POA&M) identifies tasks that need to be accomplished to mitigate risks to an information system. The POA&M is initiated by the Certifying Agent for use by the system owner, and it details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

- The *certification statement* is prepared by the Certifying Agent to provide information to the designated approving authority to permit an informed decision regarding the secure operation of the system. The statement provides a summary of the results of certification testing; highlights certification activities; records the degree to which security controls are correctly implemented and effective; identifies the level of risk to system assets and to HUD operations and personnel; states the level of compliance with statutory and regulatory requirements; and documents the certification level of the system.

- The *accreditation statement* documents the security accreditation decision from the designated approving authority. The system owner prepares the final security accreditation decision letter for the DAA with authorization recommendations, as appropriate. It is maintained by the information system owner. The accreditation statement contains the following information:

    - Security accreditation decision;
    - Supporting rationale for the decision;
    - Summarization of corrective actions required;
    - Identification of residual risks;
    - Limitations to operations; and
    - Terms and conditions for the authorization.

  The accreditation statement indicates to the information system owner whether the system is either authorized to operate or is not authorized to operate. The supporting rationale provides the information system owner with the justification for the authorizing official's decision. The terms and conditions for the authorization provide a description of any limitations or restrictions placed on the operation of the information system that must be adhered to by the information system owner. The accreditation statement is attached to the original accreditation package and returned to the information system owner.

Upon receipt of the accreditation statement and accreditation package, the system owner accepts the terms and conditions of the authorization. The system owner maintains the original accreditation statement and accreditation package on file. The DAA and OA information security officer also retain copies of the security accreditation decision letter and accreditation package. Additionally, a scanned electronic version of the accreditation statement will be provided to the HUD Enterprise IT Security Manager. The contents of security certification and accreditation-related documentation (especially information dealing with information system vulnerabilities) will be marked and protected appropriately in accordance with agency policy, and will be retained in accordance with the agency's record retention policy.

C&A Package Documentation Requirements

All accreditation packages, at a minimum, will include the documentation specified in Table 5 below.

Table 5: C&A Package Documentation Requirements

Documentation	Low SCL	Moderate SCL	High SCL
System Security Plan	✓ **(See Note 1)**	✓	✓
Technical Architecture Document			✓
Minimum Security Baseline Assessment	✓	✓	✓
Risk Assessment	✓	✓	✓
Contingency Plan **(See Note 2)**			✓
Security Test and Evaluation	✓	✓ **(See Note 3)**	✓ **(See Note 3)**
Automated Vulnerability Scan Results – General Support Systems **(See Note 4)**	✓	✓	✓
Automated Vulnerability Scan Results – Major Applications **(See Note 4)**		✓	✓
IT Security Baseline Configuration Assessment **(See Note 4)**	✓	✓	✓
Plan of Action and Milestones	✓	✓	✓
Certification Statement	✓	✓	✓
Accreditation Statement	✓	✓	✓

Note 1: The Controls Identification Section of the security plan for SCL-1 systems will consist of a *Controls Status Summary Table* and a completed *Minimum Security Baseline Assessment* (refer to Section B of the SSP Template).

Note 2: While contingency plans are generally required for HUD systems categorized as having moderate or high availability requirements, they are only required to be included in C&A Packages for High SCL systems.

Note 3: The ST&E must be performed by an independent Certifying Agent (as defined in Section 3 above).
Note 4: Will be completed as part of ST&E.

CAP Guides and Templates

This HUD C&A guidance includes a variety of other instructions, examples, and templates to aid HUD personnel in the creation of C&A documentation that meets minimum requirements. The following guidelines, templates, checklists and examples are provided:

- HUD *IT System Certification and Accreditation Inventory Guide*
- Security Plan Template
- Risk Assessment Report Template
- ST&E Plan and Results Template
- Minimum Security Baseline Assessment Template
- Plan of Action and Milestones Template
- Certification Statement and Full Accreditation Statement Template

Use of the HUD *IT System Certification and Accreditation Inventory Guide* is required, but use of templates is not. Nevertheless, they should be followed whenever possible to permit standardization across the Department.

Section 6.0 Certification and Accreditation Glossary

This glossary contains terms and associated definitions that are used throughout the HUD C&A Process. The source of the terms and definitions are provided with the definition where applicable.

Accreditation - [NIST SP 800-37] The official management decision given by a senior HUD official to authorize operation of an information system and to explicitly accept the risk to HUD operations (including mission, functions, image, or reputation), assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Accreditation Boundary - All components of an information system to be accredited by designated approving authority and excluding separately accredited systems, to which the information system is connected.

Accreditation Package - [NIST SP 800-37] The evidence provided to the designated approving authority to be used in the security accreditation decision process. Evidence includes, but is not limited to: (i) the system security plan; (ii) the assessment results from the security certification; and (iii) the plan of action and milestones.

Accrediting Authority - See Designated Approving Authority.

Authorization - See Accreditation.

Authorize Processing - See Accreditation.

Authorizing Official - See Designated Approving Authority.

Certification - [NIST SP 800-37] A comprehensive assessment of the management, operational and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Certifying agent - [NIST SP 800-37] The individual, group, or organization responsible for conducting a security certification.

Certification Package [NIST SP 800-37] - Product of the certification effort documenting the detailed results of the certification activities. The certification package includes the security plan, developmental and/or operational ST&E reports, risk assessment report, and certifier's statement.

Common Security Control – [NIST SP 800-37] A security control that can be applied to one or more HUD information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of a HUD information system where that control has been applied.

Designated Approving Authority – [NIST SP 800-37] The official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to HUD operations (including mission, functions, image, or reputation), assets, or individuals.

General Support System [OMB Circular A-130, Appendix III] - An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

Information Owner [CNSS Inst. 4009] – An official having statutory or operational authority for specified information and having responsibility for establishing controls for its generation, collection, processing, dissemination, and disposal.

Information System [44 U.S.C., Sec. 3502] [OMB Circular A-130, Appendix III] - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Owner (or Program Manager) [CNSS Inst. 4009, Adapted] - Official having responsibility for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information System Security Officer [CNSS Inst. 4009, Adapted] - Individual responsible to the DAS ISSO, designated approving authority, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program.

Major Application [OMB Circular A-130, Appendix III] - An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

Management Controls [NIST SP 800-18] - The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

Minimum Security Baseline Assessment - An evaluation of controls protecting an information system against a set of minimum acceptable security requirements.

Minor Application - [NIST SP 800-37] An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.

National Security System [44 U.S.C., Sec. 3542] - Any information system (including any telecommunications system) used or operated by HUD or by a contractor of HUD, or other organization on behalf of HUD— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Operational Controls [NIST SP 800-18] - The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).

Plan of Action and Milestones [OMB Memorandum 02-01] - A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Risk Assessment [NIST SP 800-30] - The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. A Risk Assessment is part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.

Security Authorization - See Accreditation.

Security Accreditation - See Accreditation.

Security Category [FIPS 199] - The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

Security Objective - Confidentiality, integrity, or availability of information.

Security Plan - See System Security Plan.

Security Test and Evaluation [NIST SP 800-37] - The techniques and procedures employed during a C&A process to verify the correctness and effectiveness of security controls in an IT system. There are typically two types of ST&E activities, (i.e., developmental and operational ST&E), that can be applied during the certification phase depending on where the system is in the system development life cycle.

System - See Information System.

System-specific Security Control - [NIST SP 800-37] A security control for an information system that has not been designated as a common security control.

System Security Plan [NIST SP 800-18] - Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Technical Controls [NIST SP 800-18, Adapted] - The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

User Representative - [NIST SP 800-37] An individual that represents the operational interests of the user community and serves as the liaison for that community throughout the system development life cycle of the information system.

Vulnerability [CNSS Inst. 4009, Adapted] - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.