



S T A T E O F M A R Y L A N D
DEPARTMENT OF INFORMATION TECHNOLOGY

*Information Technology
Security Certification and Accreditation Overview*

*Version 2.2
September 2008*

Table of Contents

1.0 Executive Summary	4
2.0 Background	4
3.0 Purpose	5
4.0 Scope	6
5.0 Change Process	6
6.0 Assumptions	6
7.0 State of Maryland Exceptions to NIST 800-37	7
8.0 References	8

Record of Changes

Issue	Date	Pages Affected	Description
Original Guidelines C&A	10/25/2002		
Version 2.0 - C&A Guidelines	08/16/2004	All	Replace with NIST 800-37
Version 2.1 - C&A Guidelines	3/4/2005	4	Update and correct V. 2.0
Version 2.2 - C&A Guidelines	9/2/2008	All	Updated to reflect Department of Information Technology

1.0 Executive Summary

The replacement of the State's C&A guidelines with the NIST 800-37 guidelines are based on the several factors: 1) The current guidelines are extremely labor intensive, and many agencies are not able to devote the personnel and time to the complete application of these guidelines. 2) The current guidelines are based on DOD standards, which are not always applicable to State of Maryland agencies. 3) The availability of NIST 800-37 allows for the use of an effective C&A program which utilizes the best practices from several different sources, including, but not limited to the DOD. 4) NIST will maintain 800-37 and ensure that any changes in technology or practice are reflected and the document is updated. 5) The availability of the 800 series, used in conjunction specifically with 800-37, can greatly augment an agency's security program.

The nature of NIST 800-37 is not static. The document is a living document which NIST will modify based on industry guidance as security policies and technology evolve. The decision as to accept or not accept these future changes is at the discretion of the Assistant Director of Security Department of Budget and Management, Office of Information Technology, not the individual agencies.

2.0 Background

Developing and operating Information Technology (IT) systems is a partnership between business (also known as functional) staff and IT specialists. The overall responsibility of each State of Maryland Executive Branch Agency (or Department) is protecting the systems and the information stored, processed, and communicated through those systems from inappropriate, unplanned, and unlawful disclosure, modification, destruction, or loss of availability. As such, the protection of information is a part of the partnership between the business staff and the IT specialists. A key aspect of the relationship is providing assurance that the systems and information are appropriately protected. The certification and accreditation process is a mechanism for creating that assurance.

Certification – The comprehensive assessment of the technical and non-technical security features and other safeguards of a system to establish the extent to which a particular system meets a set of specified security requirements for its use and environment.

Accreditation – Formal declaration by a Designated Approval Authority (DAA) that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

State policy for IT systems requires that all Executive Branch agencies certify and accredit the IT systems and sites under their ownership and control. The Department of Information Technology has assumed the responsibility for developing, maintaining, and revising information technology policies and standards.

All Federal Agencies are mandated to comply with the Federal Information Security Management Act (FISMA) guidelines. However, since the State of Maryland is not a Federal Agency, the state is not mandated to follow the FISMA guidelines, but may however draw upon key elements of FISMA when establishing its own policies.

The State of Maryland chose to include a security Certification and Accreditation (C&A) process as part of the IT lifecycle for state government systems. IT Security C&A programs are required of federal government departments and agencies, and a significant amount of knowledge and expertise has been amassed by the federal government with respect to programs and processes of this nature. The Maryland C&A program will model the National Institute of Standards and Technology (NIST) Document 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems. The process the State of Maryland will use when conducting a C&A effort will follow 800-37's process, which begins on Chapter 3.0, Pg. 25. The NIST maintains the 800 series, which gives detailed assistance in developing an effective security program series, which is based on Federal, DoD, Intelligence Community, State Government and industry best practices. The use of 800-37 will allow for a robust C&A program based on sound government and industry guidance. NIST draws heavily upon Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, as a foundation for 800-37. Familiarization with both NIST 800-37 and FIPS 199 will aid an agency's C&A process. The State of Maryland will take certain exceptions to NIST 800-37 and does not adopt this document verbatim. The reasons for these exceptions are based on certain roles and responsibilities for personnel defined in NIST 800-37. The state/agency may or may not have staff with the identical titles or job descriptions as those outlined in NIST 800-37. These exceptions will be outlined in section 8.0 State of Maryland Exceptions to NIST 800-37 of this document.

3.0 Purpose

The purpose of this guidance is to improve the current C&A process for the State of Maryland Executive Branch of government. This C&A process is part of the overall risk management process for IT systems and sites. The C&A process is intended to provide assurance to the managers responsible for an agency's business mission and IT infrastructure that the security risk to the systems and sites certified and accredited following this process was evaluated and determined to be at a level acceptable to those managers.

As previously stated, the State of Maryland is not a Federal agency and therefore is not bound to the FISMA guidelines, neither is it bound to the Office of Management and Budget (OMB) A-130 Management of Federal Information Resources guidelines. However, certain state agencies currently, and will in the future, have reasons for direct connection to Federal Information Systems. An example of the connection of the Maryland State Police's connection to the FBI NCIC system. Federal agencies are beginning to mandate systems with interconnections to their own information systems to have had a security certification performed on them prior to connection, or to retain a current connection. The NIST 800-37 guidance will allow a uniform format for certification and accreditation of State of Maryland systems, which will provide these Federal agencies with such a certification effort.

These guidelines are intended to enhance the risk management process for IT systems and sites. The programs and methods included will provide a formal mechanism for evaluating: how well IT systems meet information security requirements; the level of risk that remains; and, whether or not to operate those systems at that level of risk. Implementing these guidelines, as part of the practice of acquiring and operating IT systems, will ensure that these issues are given due consideration throughout the process and provide an increased level of security awareness throughout an organization. The following objectives accomplish this purpose:

- Provide a procedure for performing security certification and accreditation activities for IT systems and sites at the agency level,
- Show how the IT security certification and accreditation procedure is integrated into the Systems Development Lifecycle and IT Investment Management processes,
- Identify the roles and responsibilities for security certification and accreditation activities, and map those roles and responsibilities to typical State of Maryland Executive Branch agency positions, and
- Describe the basic outline of security certification and accreditation programs to be implemented at the agency and state levels in order to put these guidelines into practice.

4.0 Scope

These guidelines apply to all agencies of the Executive Branch of the government of the State of Maryland. Agencies are encouraged to evaluate and accredit each IT system and/or site operated by or on behalf of the agencies (including those operated by contractors).

5.0 Change Process

It is the responsibility of the Department of Information Technology to maintain this guideline document and to ensure version control. A scheduled review will occur at least annually. In addition, the Department of Information Technology will ensure this document is reviewed for impact when there are modifications to state security policies. NIST may periodically recommend changes to the existing procedures based on new technologies. These changes will enhance the overall effectiveness of the program. The Department of Information Technology will ensure that any relevant NIST recommended alterations are reflected in the State guidelines.

Changes to this document will be recorded on the Record of Changes Page immediately following the Table of Contents. The Department of Information Technology will distribute revisions to the Executive agencies via a link on the Department of Information Technology web site.

6.0 Assumptions

The following assumptions were made during the preparation of this document:

- These guidelines will be implemented as part of a comprehensive Information Technology Security program, with the appropriate policy, standards, guidelines, and procedures.
- The State will maintain a statewide C&A program as part of the state's total information security program.
- These guidelines will be implemented as part of an agency's C&A program, which is itself part of the agency's total information security program.
- The state and agency information security programs will define and assign security responsibilities and duties to appropriate individuals involved in the lifecycle of IT systems.
- Certain IT Security Certification roles, such as the Certifier and Certification Team members, require specialized knowledge, skills, and training.
- Appropriate skills and training will exist among an agency's personnel to interpret and implement the process described in this document.
- The roles and responsibilities identified in this document will be appropriately assigned to individuals with the capacity to carry them out.
- Standardized baseline requirements and baseline controls exist in order to provide a starting point for requirements analysis and a basis for evaluating systems and sites using the process in this document.
- The Baseline Level Security Requirements (BLSR's) will continue to be based on the BLSR's provided in NIST 800-53.

7.0 State of Maryland Exceptions to NIST 800-37

With the replacement of the current State of Maryland C&A guidelines by the NIST 800-37, it is critical that all individuals understand their role in the process and what information is required. The current NIST 800-37 outlines roles and responsibilities of key personnel in detail. The State of Maryland takes exception to certain aspects of NIST 800-37 and dictates the following exceptions be taken to the guidance:

- Chief Information Officer (CIO) role (NIST 800-37, Pg. 12): The CIO for the agency undergoing the C& A will most likely act as the Designated Approving Authority (DAA). However, the DAA role and responsibilities may be formally delegated to another senior management official. The responsibility of the DAA will be maintained by the DAA and not delegated.
- Authorizing Official Designated Representative role (NIST 800-37, Pg.13): The State of Maryland C&A Process will not involve this specific role. The responsibility of the Designated Approving Authority (DAA) will be maintained by the DAA and not delegated.
- Senior Agency Information Security Officer (NIST 800-37, Pg. 13)_role: The State of Maryland C&A process will not involve this specific role. If an agency has more than one Information security officer responsible for the system being accredited, the agency will assign one of these personnel as the Information Security Officer for the C&A effort. This will allow for a single point of contact between the security management of the system and the Certification Agent.
- User Representative (NIST 800-37, Pg. 15) role: The State of Maryland C&A process will not utilize a user representative unless it is determined by the

Certification Agent and the DAA that this individual offers a unique perspective on the system's security posture critical to the accreditation effort.

- Supporting Documentation (NIST 800-37, Pg. 22): Per NIST 800-37, all available documentation will be compiled into a documentation package, which will then be submitted by the information system owner and the security officer directly to the DAA for review. Under the State of Maryland C&A guidance, the chain of custody for the documentation package will be altered in the following manner: The information system owner and the security officer will submit the documentation package to the certification agent, who after review and comments will submit a certification decision along with the documentation package to the DAA for a final accreditation decision.
- Continuous Monitoring (NIST 800-37, Pg. 23): The continuous monitoring results should also be considered with respect to any necessary updates to the system security plan and to the plan of action and milestones, since the authorizing official, information security officer, and information systems owner will be using these plans to guide future security certifications and accreditation activities. The certification agent is not responsible for the continuous monitoring of the system or the updating of its supporting security documentation.
- Security Certification and Accreditation for Low Impact Systems (NIST 800-37, Pg. 26), (FIPS 199, Pg 6.): The State of Maryland will not perform certification and accreditation on Low Impact Systems. A Low Impact System based on FIPS 199 classification with regards to Confidentiality, Integrity, and Availability is described as:
 - Confidentiality- The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.
 - Integrity- The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.
 - Availability-The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals

8.0 References

The NIST 800 series has been mentioned as an augmentation to an agencies current security program. In order to be compliant with 800-37, an organization must maintain a System Security Plan, Disaster Recovery Plan, Effective Security Training Program, Incident Handling Procedures and other varied documented policies. The locations of the 800 series documents that may aid in becoming compliant are listed below.

- Interconnection of Information Systems: NIST 800-47
<http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf>
- Standards for Security Categorization of Federal Information Systems: FIPS 199
<http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>
- Developing a System Security Plan: NIST 800-18
<http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf>
- Computer Security Incident Handling Guide: NIST 800-61
<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

- Security in the Information System Development Life Cycle: NIST 800-64
<http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf>
- Recommended Security Controls for Federal Information Systems: NIST 800-53
<http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf>
- Wireless Network Security: 802.11, Handheld Devices: NIST 800-48
http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
- Guideline on Network Security Testing: NIST 800-42
<http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf>
- Guidelines on Firewalls and Firewall Policy: NIST 800-41
<http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf>
- Creating a Patch and Vulnerability Management Program: NIST 800-40
<http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>