National Information Assurance Partnership /Common Criteria Evaluation and Validation Scheme

Publication #2

Quality Manual and Standard Operating Procedures

January 2020
Version 5.0

All correspondence in connection with this document should be addressed to:

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme
9800 Savage Road, Suite 6940
Fort George G. Meade, MD 20755-6940
E-mail: niap@niap-ccevs.org
https://www.niap-ccevs.org/

Amendment record

Version	Date	Description
Draft 1.5	May 2000	Initial release.
2.0	8 September 2008	Complete revision based on current operations
3.0	May 2014	Updates
4.0	February 2016	Updates
5.0	January 2020	Updates to reflect minor program changes

(Page intentionally left blank)

Table of Contents

1 Introduction

The National Information Assurance Partnership (NIAP), Common Criteria Evaluation and Validation Scheme (CCEVS), or Scheme, was originally established by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to validate conformance of Information Technology (IT) products to international standards. NIAP, now solely part of NSA, oversees the evaluations performed by Common Criteria Testing Laboratories (CCTLs) on information technology products against the Common Criteria for Information Technology Security Evaluation (CC).

The principal participants in the NIAP program are the:

- **Sponsor**: The Sponsor may be a product developer, a value-added reseller of an IT security-enabled product, or another party that wishes to have a product evaluated. The sponsor requests that a CCTL conduct a security evaluation of an IT product.

- **Common Criteria Testing Laboratory (CCTL)**: The CCTL is a commercial testing laboratory accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by NIAP to perform security evaluations against the CC using the Common Methodology for Information Technology Security Evaluation (CEM).

- **National Information Assurance Partnership (NIAP**): NIAP is the government organization established by NSA to maintain and operate the Scheme for the U.S. Government and to oversee and validate the evaluations performed by the CCTLs.

1.1 Purpose

This document satisfies the NIAP requirement for a quality manual. All NIAP standard operating procedures are either contained in this document or included by reference in other NIAP documents (see section 1.2). This *living document* is updated as NIAP policies and procedures evolve. Any NIAP standard operating procedures (SOPs) are also periodically reviewed and updated.

The primary audience of this document is the NIAP staff. Others who may find it useful include members of a CCTL staff, security target (ST) authors, product developers, and sponsoring organizations.

1.2 Organization and Scope

This document is part of a series of technical and administrative NIAP publications describing how the scheme operates. It consists of several chapters and supporting annexes as defined in the Table of Contents and complements or references other NIAP publications and documents used in the operation of the NIAP. These other publications include:

Publication #1: *Organization, Management, and Concept of Operations*

Publication #2: *Quality Manual and Standard Operating Procedures*

Publication #3: *Guidance to Validators*

Publication #4: *Guidance to CCEVS Approved Common Criteria Testing Laboratories*

Publication #5: *Guidance to Sponsors*

Publication #6: *Assurance Continuity: Guidance for Maintenance and Re-evaluation*

Other documents that provide guidance to NIAP, such as Common Criteria, NIST and ISO publications, are also referenced. The reader of this document must be familiar with these reference documents to gain a clear understanding of the NIAP quality guidance provided herein. NIAP related publications and information are available on the NIAP web site https://www.niap-ccevs.org.

2 NIAP and Quality System Overview

2.1 NIAP Overview and Legal Status

NIAP is the government entity responsible for U.S. implementation of the Common Criteria, including management of the Scheme. NIAP operates in accordance with:

- Scheme Publication #1 - Organization, Management and Concept of Operations;
- ISO/IEC Guide 17065 –Requirements for Bodies Certifying Products, Processes, and Services; and
- Common Criteria Recognition Arrangement (CCRA).

References to these documents throughout this publication will be document with the document short title, and the applicable paragraph number(s) within brackets (e.g., [CCRA C.5b]).

NIAP was established under the following authorities:

- Computer Security Act of 1987 (Public Law 100-235, Jan 8, 1988) - Provides for a computer standards program within the NIST. This program provides for government-wide computer security, and the security-related training of persons involved in the management, operation, and use of Federal computer systems, and for other purposes. The Computer Security Act, as amended by FISMA and now with OMB oversight, provided a role for NSA to assist NIST with establishing standards for non-national security systems. Under Section 2, NIST shall:
  - Develop technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems as defined in the Act; and
  - Draw on the computer system technical security guidelines of the NSA in this regard, where appropriate.

- The NIST and NSA Memorandum of Understanding (MOU) dated March 1989 (to implement P.L. 100-235). The MOU defines terms for NSA to provide assistance to other U.S. Government agencies.

- Letter of Partnership, National Security Agency and National Institute of Standards and Technology, dated 22 August 1997 (forming the NIAP).

- National Voluntary Laboratory Accreditation Program (NVLAP) Laboratory Accreditation Program (LAP) for Information Technology (IT) Security Testing, dated February 2006.

- Common Criteria Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, dated July 2014.

- E-Government Act of 2002 (Public Law 107-347, Dec 17, 2002). (The Federal Information Security Act was part of P.L. 107-347) mandates that the NIST develop security standards for Federal (non-NSS) systems.

- National Security Directive (NSD) No. 42 (National Policy for the Security of National Security Telecommunications and Information Systems, dated July 5, 1990) and implementing documents establishes the Committee on National Security Systems (CNSS) and grants NSA the authority to evaluate products being used on or with national security systems.

- Committee on National Security Systems Policy (CNSSP) No. 11 (National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products, dated June 2013) specifies the responsibilities of NIAP in approving processes for the evaluation of COTS products when they are to be used to protect information on NSS.

[CCRA C.3d, C.9]

NIAP's responsibilities are to:

- Establish and implement policies and procedures for the operation of the scheme, and ensure the policies and procedures are adhered to;

- Document and publicize the organization, policies, and procedures of the Scheme;

- Approve CCTL participation in the Scheme and publicize the approved CCTLs on the NIAP Approved Common Criteria Testing Laboratories List;

- Monitor the performance of participating CCTLs and their adherence to, application of, and interpretation of the CC and the CEM;

- Add or Remove a CCTL from the NIAP Approved CCTLs List once a laboratory obtains accreditation or fails to meet the terms and conditions of the scheme;

- Notify to the community of any changes to the NIAP Approved CCTLs List including additions or withdrawals of CCTLs from the scheme and any modifications to the scope of a laboratory's accreditation;

- Ensure that appropriate procedures are in place within the scheme to protect sensitive or proprietary information relating to IT products under evaluation, and that those procedures are routinely followed;

- Provide advice, guidance, support, and standards for training to CCTLs as required;

- Review evaluation technical reports from CCTLs to ensure that the conclusions are consistent with the evidence presented and that the CC and the CEM have been correctly applied;

- Ensure consistency of CCTL evaluations across the Scheme with the use of approved Protection Profiles (PPs) generated by experts in Technical Communities;

- Seek guidance from industry experts, (e.g., consumer groups, IT product technical community, testing laboratories, researchers, standards groups), when answering technical questions, resolving disputes, addressing challenges, or making critical decisions regarding any aspect of the scheme;

- Issue CC certificates for products successfully evaluated and validated by the scheme;

- Publish and maintain a Product Compliant List (PCL) of all successfully evaluated and validated products, along with their respective Security Targets (STs) and validation reports;

- Promote the integrity of the CC certificates and ensure the CC and NIAP logos are used in compliance with NIAP CCEVS Publication #5, Annex D;

- Ensure that the interests of all parties participating in scheme activities are given appropriate consideration;

- Arbitrate disputes arising in the context of the scheme and provide procedures for appeal or reconciliation;

- Approve press releases or similar statements relating to the scheme;

- Maintain a system for creating, storing, accessing, archiving, and disposing of scheme records used to document NIAP activities;

- Ensure NIAP and CCRA procedures/processes are consistent with U.S. Government policies and work with the appropriate policy offices (DoD, CNSS, etc.) when Policies require modifications;

- Prioritize, establish, lead, and manage technical communities; for the development or revision of Protection Profiles (PPs);

- Facilitate the development of new and revised Protection Profiles, working with Technical Communities and NSA information assurance Subject Matter Experts and promulgate those PPs;

- Liaise with international schemes to ensure a robust collection of evaluated products and a consistent way forward within the Common Criteria Recognition Arrangement (CCRA).

2.1.1 NIAP Management

A Director is selected by NSA management to lead and oversee all NIAP activities. The certificate-issuing authority is the NIAP Director.

The NIAP certificate issuing authority provides final decisions on issuance and revocation of CC certificates, official signatures on CC certificates, changes in NIAP policy, and resolution of issues with the CCRA partners. They are referred to as signatories throughout the rest of this document.

2.1.2 NIAP Personnel

NIAP employs both technical and operational administrative staff in order to provide the full range of NIAP services. NIAP entrusts the accreditation of CCTLs to NVLAP and depends on the CCTLs for the evaluation of products. NIAP contracts portions of the validation and technical oversight functions to organizations with no financial or legal interests in the outcome of the validations.

All employees, contractors, and others that provide services to NIAP are bound by the policies, procedures, and other conditions set by NIAP and described in this document. Adherence to these policies and procedures is a condition of employment. Any deviation, without the written consent of the NIAP Director, is grounds for employee dismissal or termination of the contract or agreement.

[CCRA C.2]

2.1.3 NIAP Organization

NIAP is organized to effectively meet its mission goals, and assure the implementation of its policies. NIAP management functions are comprised of the following positions: Director, Deputy Director, Technical Lead, Quality Manager, Technical Oversight Team, Business Manager, Contracts Manager, and Data/Records Manager. The organizational chart is depicted in Figure 2.1, followed by a brief summary of each position. A more detailed description of the NIAP roles and responsibilities is defined in Section 4.

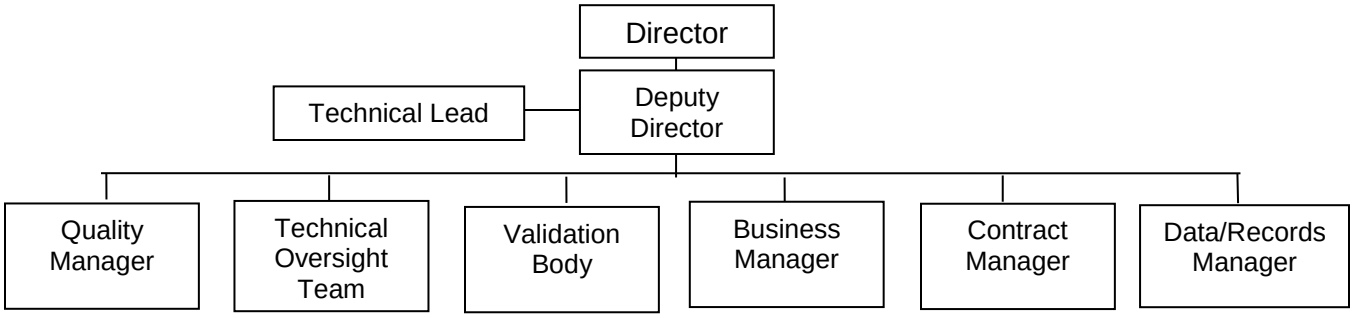

Figure 2.l: NIAP Organizational Chart

[CCRA C.3]

2.1.3.1 Position Descriptions

- Director
  The NIAP Director is the certificate issuing authority and provides strategic direction for the overall CCEVS program and day-day-oversight and leadership to NIAP.

- Deputy Director
  The Deputy Director provides direction to the Scheme. The Deputy Director works with the Technical Lead in establishing a way forward for NIAP activities.

- Technical Lead
  The NIAP Technical Lead ensures overall effective and efficient operation of NIAP by working with the Deputy Director to provide technical direction to the NIAP Director. The Technical Lead also provides guidance to validators and CCTLs. The Technical Lead also fills in for the Director or Deputy Director when they are unavailable.

- Quality Manager
  The Quality Manager is responsible for ensuring the day-to-day operation of the NIAP program conforms to the quality system described in this scheme publication.

- Technical Oversight Team
  The Technical Oversight Team is responsible for all technical aspects of NIAP operations, assigning Validation teams for CC evaluations, and providing direction and oversight to validators and senior validators in the performance of their duties. This team also provides an interface to the Technical Community for PP development.

- Validation Body
  Each individual performing validation activities will be designated as a validator trainee, lead validator, or senior validator. A particular validator progresses through each validator designation as their experience and proficiency in performing CC validations improves and as they are approved by NIAP Management.

- Business Manager
  The NIAP Business Manager will interface with the NSA budget and procurement offices to ensure NIAP budgeting and finance needs are met.

- Contracts Manager
  The NIAP Contracts Manager will interface with appropriate NSA Contract Officers and contractors to ensure all contracts, subcontracts, working agreements, and assessments of contractors are properly executed and operating. (NOTE: for the purpose of this document, any external (non-NSA) organization performing work for the NIAP through contracts or working agreements are all referred to as contractors).

- Data/Records Manager
  The Data/Records Manager is responsible for the Data/Record keeping operation of the NIAP and for monitoring its performance. This includes procedures for creating, storing, accessing, archiving and disposing of NIAP records used to document NIAP activities.

2.1.4 Funding Source

The NSA is responsible for providing sufficient resources for the NIAP to carry out its assigned responsibilities. The NSA provides all resources and funding for the operation of the NIAP.

[CCRA C.1, C.3]

2.1.5 Complaints and Appeals

Persons or organizations affected by NIAP decisions and actions have the right to file a formal complaint and appeal the decision when they believe NIAP actions have not been conducted according to the rules or standards of NIAP, or the actions have resulted in unfair treatment of persons participating in or who are affected by NIAP activities. A person or organization disagreeing with a NIAP decision on a complaint may appeal the decision for review by the NIAP Director.

NIAP may enlist the guidance of technical, regulatory and other relevant experts to resolve complaints or appeals. NIAP may also form an independent arbitration panel to resolve the dispute. Procedures for filing and resolving complaints and appeals are described in Section 3.4, Complaints and Appeals.

[CCRA C.12]

2.1.6 Public Information Dissemination

NIAP will make information about its operation and services available to the public via its website. All NIAP information for public consumption will be published and distributed to the public prior to the effective date of the change using the procedures described in Section 5.2, Document Control. The NIAP Director or designee must approve all information about NIAP activities before it is disseminated to the public. Information about contacting or retrieving information from the NIAP may be found on the NIAP website.

[CCRA C.11]

2.1.7 Common Criteria Recognition Arrangement (CCRA) Participation

NIAP standard operating procedures have been developed to satisfy its CCRA obligations including:

- Accepting definitions in the CCRA
- Co-developing and adopting common test methods and interpretations

- Uploading required NIAP documentation to the CCRA portal
- Protecting proprietary information obtained from CCRA participants
- Ensuring evaluations are conducted appropriately by providing sufficient oversight.

[CCRA]

2.2 NIAP Quality System Overview

The NIAP Quality System is designed to ensure security evaluation and validation services for both government and industry meet the quality and functional requirements of the CCRA and ISO/IEC17065. The major components of the Quality System include policy, personnel organization, and functional organization. For additional detail see Section 2.2.1, NIAP Policies and Section 4, NIAP Personnel and Qualifications.

2.2.1 NIAP Policies

In an effort to meet the requirements of the CCRA and to promote quality, the NIAP has adopted policies that apply to all persons performing validation activities on behalf of the NIAP. Section 2.2.1, NIAP Policies, describes the NIAP Quality Policy, Information Confidentiality Policy, and the Records Management Policy.

2.2.1.1 NIAP Quality Policy

A Quality Policy defines the overall intentions and direction of an organization with regard to quality and is endorsed and expressed by upper-level management. The NIAP quality policy is outlined below.

NIAP will:

- Provide its services in a non-discriminatory manner.
- Protect proprietary information.
- Implement and maintain:
    - A quality system for the operation of the NIAP that includes compliance with the requirements of both the CCRA, as enumerated in the NIAP, and ISO/IEC17065.
    - Procedures to assure the impartiality, objectivity, and integrity in all NIAP activities.
    - Procedures that assure consistency across all evaluations.
- Ensure timely and accurate reporting of validation results to the public.
- Monitor the use of NIAP issued CC certificates and revoke NIAP CC certificates or pursue legal actions against those that abuse the privileges granted or bring embarrassment to the NIAP by use of the certificate and privileges associated with the certificate.
- Assure the adequacy and relevancy of NIAP skills and expertise.

[CCRA C.1, C.2, C.4, C.9]

2.2.1.2 NIAP Information Confidentiality Policy

NIAP is responsible to ensure the confidentiality of information obtained in the course of NIAP activities at all levels of the organization, including committees and external bodies or individuals acting on its behalf. The supplier of information is responsible for marking/labeling all proprietary information delivered to NIAP. Any information designated as proprietary must not be disclosed, copied, reproduced, or otherwise made available in any form to any other person not acting on behalf of the NIAP, except as such information may be subject to disclosure under the Freedom of Information Act (5U.S.C 552).

NIAP will use its best efforts to protect information designated as proprietary from unauthorized disclosure. NIAP will not be liable for the disclosure of information designated as proprietary that, after notice to and in consultation with the supplier, NIAP determinations may not lawfully be withheld or a that court of competent jurisdiction requires disclosed.

All persons performing work for NIAP are required to sign non-disclosure agreements avowing they understand and will comply with the proprietary information confidentiality policy described above and the NIAP Information Security Policy, as defined in Publication #3, Annex F. This applies to both employees and contractors.

[CCRA C.10]

2.2.1.3 NIAP Records Management Policy

NIAP is responsible for maintaining accurate records to demonstrate NIAP procedures have been effectively implemented and to ensure the traceability, repeatability, and reproducibility of evaluations and validations. Records generated, modified, or deleted by either NIAP personnel or by persons performing work for the NIAP must comply with the NIAP Records Management Policy as documented below.

- Records should be:
    - Clearly identified and traceable to the procedure(s) involved or to the quality system activity they document.
    - Filed, indexed, and maintained in a manner that provides for safe storage and ready access or retrieval.
    - Accurate and truthful representations of actual events and documented in a timely manner.
    - Dated and clearly identify the person(s) generating or modifying the records as specified in the applicable procedures.
- Personnel involved in collecting data for records should be provided instructions and training to the degree necessary to ensure the records are generated correctly.
- Any person or organization performing work for NIAP must make those records dealing with evaluation or validation activities available to NIAP.

[CCRA C.6]

3 Quality Management

NIAP is required to operate and maintain quality in NIAP evaluations and certificates. To accomplish this, NIAP has designated a Quality Manager, promoting quality in NIAP personnel; developed quality documentation, procedures for internal audits, procedures for management reviews, guidance on subcontractor management; and established an arbitration process for internal and external issues. NIAP has assigned a Functional Manager, generally the Deputy Director, for each quality function to work with the Quality Manager to maintain quality. Each of these quality elements is described below.

3.1 Quality Manager

The Quality Manager ensures NIAP policies are implemented and maintained by NIAP. The Quality Manager is responsible for:

- Ensuring all personnel understand their role in achieving quality in NIAP
- Maintaining quality documentation
- Organizing and coordinating internal audits
- Coordinating management reviews of the NIAP quality system
- Reporting on the performance of the quality system to NIAP management
- Tracking and monitoring the status of complaints, disputes, appeals, and corrective and preventive actions

3.1.1 Promoting Quality among NIAP Personnel

The Quality Manager is also responsible for ensuring all personnel are equipped to carry out their individual roles according to the NIAP quality system. To accomplish this, the Quality Manager:

- Ensures all personnel meet the qualifications of their assigned roles.
- Provides periodic NIAP Standard Operating Procedure training courses and seminars.
- Ensures all quality documentation is available to all personnel.

3.2 Quality Documentation

NIAP has documented its quality system. This documentation is available to all NIAP staff. The Quality Manager is responsible for periodic audits and reviews of quality documentation to ensure it is understood, implemented, and maintained according to the document control procedures in Section 5.2, Document Control.

3.3 Internal Audits

NIAP has established the following activities for performing internal audits of its own quality procedures. The purpose of identifying these activities is to ensure all internal audit activities are performed in a consistent manner, audit results are adequately reported, and any follow-up activity or corrective action is taken.

NIAP auditing activities include the following:

1. The Quality Manager, or designee, will develop and update an internal audit schedule to perform an audit of each quality system function. The purpose of the audit is to verify NIAP continues to comply with its quality system procedures. The schedule will contain the date of the audit and the NIAP functions to be audited. Ad-hoc audits may also be scheduled to address problems identified by employees, external inputs, or to take corrective actions.

2. For each audit, the Quality Manager will:

- Identify or review previously identified objectives or goals for each audit.
- Establish an audit team and designate a team leader.
- Develop an audit checklist and provide assistance to audit team leaders in developing specific checklist items for each audit.
- Ensure each audit is conducted according to NIAP procedures and is performed when scheduled.

3. Auditor(s) shall be properly trained and verified to be free from conflicts of interest with the target of the audit. In preparation for the audit, auditor(s) shall review the audit objectives, the relevant quality system procedures, and any other information that would be helpful in conducting the audit.

4. Auditor(s) will notify the NIAP Functional Manager(s) who will potentially be affected by the audit one week prior to initiation of the scheduled audit (NOTE: ad-hoc audits will not provide a notification).

5. On the first day of the audit, a meeting shall be held with the appropriate Functional Manager(s) to explain the objectives and procedures of the audit.

6. Audit findings will be recorded in an audit report. The audit report shall contain all findings and observations made by the auditor(s). Draft and final versions of audit reports will be given to the Quality Manager and appropriate Function Manager(s) for review and distribution.

7. An exit meeting will be held with those involved in the audit to convey the findings of the audit.

8. The results of the audit and exit meeting will be documented in the audit report and the audit report will be placed in NIAP records control for a period of five years. All corrective actions or other follow-up activities identified in the audit report will be coordinated with the Quality Manager or designee.

3.3.1 Management Reviews

NIAP management will perform a formal evaluation of the NIAP quality system and quality policy once per year, at a minimum.

Management Review meetings will be held at least annually. Minutes from each meeting will be prepared and distributed by the review designee to NIAP management, the Quality Manager, and all Functional Area Managers within one week following the meeting. Management Review meetings will address but are not limited to a review of the:

- Quality Policy and other quality documentation
- Quality System
- The organizational structure and quality infrastructure
- Feedback surveys
- Training plans
- Personnel reviews
- Internal audit results
- Functional area management reviews
- Nonconformity/deficiencies and preventative/corrective actions
- Identification and prioritization of upcoming audits
- Next fiscal years' plan of action

Management Review minutes and any related documents will be placed in NIAP document and records control for a period of five years by the review board designee.

NIAP conducts two types of management reviews for quality: Functional Area Management Reviews and NIAP Management Reviews.

Functional Area Management Reviews are reviews conducted within the NIAP for a specific activity (e.g., training or document control). Functional Area Management Reviews can be either mandatory or voluntary. Mandatory reviews occur as part of the Quality Manager's quality system review whereas voluntary reviews are conducted by the appropriate Functional Manager to determine the status of quality for an individual activity.

NIAP Management Reviews cover the entire NIAP as a single entity and draw on the results of Functional Area Management Reviews.

3.3.1.1 Functional Area Management Review

A Functional Area Management Review is conducted in a systematic manner using a formal agenda. The review agenda should include the following, as appropriate:

- Evaluation of results of internal audits or audits conducted by other bodies
- Evaluation of complaints received since the last management review

- Evaluation of corrective action activities since the last management review
- Results from any customer surveys conducted or other customer feedback
- Assessment of needs to update Standard Operating Procedures
- Matters arising from the previous review
- Adequacy of NIAP staff and equipment
- Staff training
- Development of corrective actions (if a need is identified during the review)

Actions arising from the review should be documented by the functional area review designee. This person is assigned to the Functional Manager of the area where the problem or nonconformance exists and is assigned a completion date, preferably by the Functional Manager or the Quality Manager. The results of management reviews are documented by the review board designee and placed under NIAP document and records control for a period of five years.

[CCRA C.13]

3.4 Complaints and Appeals

NIAP provides a process for dealing with complaints and appeals that originate either internally or externally. The process applies, but is not limited to:

- NIAP actions, decisions, approvals, or staff assignments;
- NIAP customers and consumers;
- Internal quality system problems detected by NIAP staff members;
- CCTLs, candidate CCTLs, CCTL customers;
- Unresolved issues occurring during PP or product evaluations.

The NIAP Director is responsible for ensuring all complaints and appeals are responded to promptly and any required corrective actions are implemented in a timely manner.

3.4.1 Complaints

Complaints are written expressions of dissatisfaction regarding the quality of NIAP services provided to external or internal customers or a claim that either NIAP or a CCTL has acted improperly. Written complaints should be submitted to the NIAP Director.

NIAP will perform the following tasks when a complaint is received:

1. Place the complaint under NIAP document control and records management, recording the date of receipt

2. Forward a copy of the Complaint Record to the Quality Manager for review and processing

3. Forward a copy of the Complaint Record to the appropriate Functional Manager who is responsible for the activity identified in the complaint.

If the complaint is judged to be the result of a minor nonconformity, the Quality Manager notifies the complainant that no action is being taken and informs the complainant of their right to appeal.

If the complaint is judged to be a potentially serious nonconformity, the Quality Manager:

1. Issues a request to the responsible Functional Manager for an investigation into the issue(s) identified in the complaint

2. Issues a request to the responsible Functional Manager for the necessary corrective action(s) to be taken

3. Notifies the complainant that action is being taken

The Functional Manager to whom the complaint is assigned performs the following tasks:

1. Investigates the complaint

2. Seeks the aid of independent and impartial technical experts to help resolve technical disagreements

3. Establishes a plan and course of action to be taken to resolve the complaint

4. Reviews the plan and course of action with the Quality Manager

5. Updates the plan and course of action based on suggestions from the Quality Manager

6. Notifies the complainant of the planned decision and course of action for resolving the complaint

7. Implements the course of action to resolve the complaint

8. Notifies the Quality Manager when the complaint is resolved

9. Forwards copies of the response and any other documentation pertaining to the resolution of the complaint to the Quality Manager

Once received, the Quality Manager reviews the complaint resolution and decides to either close the complaint or request further action from the Functional Manager. When the complaint is closed, the Functional Manager responds to the complainant in writing within three business days. Finally, after the complainant has been notified, all documentation and records pertaining to the complaint resolution is forwarded to the

Quality Manager who places the complaint documentation under NIAP document and records control.

3.4.2 Appeals

If a complainant (also referred to as appellant) disagrees with the NIAP decision on a complaint and is unsuccessful in achieving an acceptable reconsideration of the issue, the complainant may file a formal appeal.

All formal appeals shall be made in writing to the NIAP Director within 30 calendar days after notification of a NIAP decision. In response to the appeal, NIAP performs the following:

1. A copy of the appeal documentation is forwarded to the NIAP Quality Manager who places the appeal documentation in NIAP document and records control for a period of five years. In order to formulate a final decision, the Director may enlist the guidance of technical, regulatory, or other relevant experts when necessary, or may form an independent arbitration panel. The Director has 30 days to reach a decision on the appeal.

2. Upon reaching a decision, the Director notifies the appellant of the outcome of the appeal, in writing, and forwards a copy of the decision and notification to the NIAP Quality Manager. The Quality Manager places the decision in NIAP document and records control for a period of five years.

3. If the appellant does not agree with the Director's decision, a re-appeal may be made in writing to the NIAP signatories for resolution. In developing a resolution the NIAP signatories may enlist the guidance of technical, regulatory and other relevant experts when necessary or form an independent arbitration panel for a resolution.

4. When an appeal is submitted to the NIAP signatories, a copy of the appeal documentation is forwarded to the NIAP Quality Manager who places the appeal documentation in NIAP document and records control for a period of five years.

5. Upon reaching a final decision, the NIAP signatories notify the appellant in writing through the NIAP Director of the outcome of the re-appeal. A copy of the resolution and notification will be forwarded to the NIAP Quality Manager. The Quality Manager places the decision in NIAP document and records control for a period of five years.

6. A written copy of the resolution is sent to the appellant, at which time the complaint decision will be considered final.

[CCRA C.12]

3.5 Quality Management Records

This section lists the records required to support the traceability and integrity of the Quality Management procedures.

3.5.1 Quality Manager Records:

Statement of who the quality manager is

3.5.2 Quality Training Records:

Training courses, seminar descriptions, and notice form

3.5.3 Quality Documentation Records

- Quality document list
- Quality documents

3.5.4 Internal Audit Records

- Audit
  - Schedule
  - Objectives and checklists for each audit
  - Team lists and verification of freedom from conflict of interest
  - Notification forms
  - Reports
  - Exit meeting findings reports
- Document and record control forms for appropriate items

3.5.5 Management Review Records

- Review
  - Schedule
  - Meeting notifications with agenda
  - Meeting minutes
- Document and record control forms for appropriate items

3.5.6 Complaint and Appeal Records

- Complaints
- Complaint decisions
- Complaint decision notifications
- Corrective actions
- Appeals
- Appeal decisions
- Appeal decision notifications

4 NIAP Personnel and Qualifications

NIAP staff members shall be composed of NSA personnel. NIAP will coordinate with the respective NSA personnel offices to process, recruit, hire, and train new staff members. The NIAP Director will work with the NSA Personnel Manager to ensure that NIAP policies and needs for recruiting, hiring, and training are met.

4.1 Personnel

The NIAP Director is responsible for defining recruitment and hiring needs to meet NIAP staffing requirements, and ensuring the staff has the resources to effectively perform in their assigned roles. Along with meeting technical and managerial requirements, all candidate NIAP personnel must agree to follow the policies of NIAP (e.g., be fair and impartial, protect proprietary information, and strive to avoid conflicts of interests).

The NIAP Director must complete the following activities for recruitment, hiring, and indoctrination of newly assigned personnel:

1. Specify and approve technical requirements for recruitment

2. Prepare and approve written criteria for recruitment

3. Identify potential candidates

4. Evaluate candidate applications and determine candidate rankings

5. Select the best qualified candidates

6. Provide written notification of selection to candidates

7. Arrange for hiring and reassignment of candidates

8. Ensure newly assigned personnel:

    a. Sign non-disclosure agreements and conflict-of-interest forms

    b. Are given a copy of the description of their role in the NIAP

    c. Are given the necessary resources to carry out the responsibilities described in their NIAP role

    d. Understand that they are required to be impartial, objective, and will avoid conflicts of interest in performing their NIAP roles

[CCRA C.2, C.4, C.7]

4.2 Qualifications

NIAP staff members must be competent in the NIAP functions they undertake. Information on the relevant qualifications, training, and experience of each member of the staff is to be maintained by NIAP and kept up-to-date. Personnel must have access to clear, up-to-date, documented instructions pertaining to their duties and responsibilities. If work is contracted to an outside body, NIAP is to ensure the personnel carrying out the contracted work meet the applicable qualifications.

Personnel qualifications must align with the roles described in Section 2.1.3, NIAP Organization, of this document. Experienced personnel will be selected for the role when such personnel are available. However, specific qualifications can either be acquired by formal training and/or on-the-job training (OJT). When OJT is used, junior personnel will be paired with senior personnel until the necessary expertise is obtained.

This section identifies the personnel and qualifications required to fulfill NIAP functions.

4.2.1 NIAP Director

The Director, NIAP, ensures overall effective and efficient operation of the NIAP by providing strategic direction to the NIAP functional managers and overseeing day-to-day operations within the NIAP.

4.2.1.1 Responsibilities include:

- Defining NIAP personnel requirements
- Determining NIAP personnel training requirements
- Approving NIAP personnel training request
- Approving changes to the NIAP and the NIAP Quality Management System
- Representing the United States at International CC Committee and Board meetings
- Rendering final decisions for NIAP disputes, complaints, and appeals
- Ensuring the NIAP is staffed and resourced to meet its objectives

4.2.1.2 Minimum Qualifications:

The NIAP Director requires extensive knowledge of IT, IT security, human resources management, project management, program management, and has business acumen and leadership competencies acquired through a combination of formal education, training, and relevant job experience.

4.2.2 NIAP Deputy Director

The Deputy Director provides direction to the scheme. The Deputy Director works with the Technical Lead in establishing a way forward for NIAP activities.

4.2.2.1 Responsibilities include:

Assisting the NIAP Director in his/her responsibilities

4.2.2.2 Minimum Qualifications:

The Deputy Director requires extensive knowledge of IT, IT security, human resources management, project management, program management; and has business acumen and leadership competencies acquired through a combination of form education, training, and relevant job experience.

4.2.3 NIAP Technical Lead

The NIAP Technical Lead ensures overall effective and efficient operation of NIAP by providing technical direction to the NIAP Director and providing guidance to validators and CCTLs.

4.2.3.1 Responsibilities include:

- Defining NIAP personnel technical requirements
- Recommending changes to the NIAP and the NIAP Quality Management System
- Representing the United States at International CC Committee and Board meetings in lieu of the NIAP Director
- Recommending final decisions for NIAP disputes, complaints, and appeals

4.2.3.2 Minimum Qualifications:

The NIAP Technical Lead must possess a Bachelor's degree in computer science, information systems, computer/electrical engineering, mathematics, or equivalent knowledge acquired through relevant work experience. The Technical Lead is required to have comprehensive knowledge of IT security evaluation or certification principles, and possess extensive experience (at least two years) in the CC and/or CEM, acquired by direct involvement with the development and/or application of the CC and/or the CEM.

4.2.4 Quality Manager

The NIAP Quality Manager ensures the NIAP program is operating in accordance with the quality system functions and that the procedures for each function are explicitly defined and can be audited.

4.2.4.1 Responsibilities include:

- Ensuring implementation of the quality management system procedures
- Conducting internal audits and management reviews to assess policy compliance and effectiveness in all functional areas
- Reporting to NIAP authorities on the performance of the quality system
- Maintaining quality system documentation
- Maintaining quality management records

4.2.4.2 Minimum Qualifications:

The Quality Manager requires extensive knowledge of quality management and quality programs, and a good understanding of IT and IT security acquired through a combination of formal education, training, and experience.

4.2.5 Technical Oversight Team

The Technical Oversight Team, composed of the NIAP Technical Lead and senior validators, is responsible for all technical aspects of NIAP operations, assigning Validation teams for CC evaluations, and providing direction and oversight for validators and CCTLs in the performance of their duties.

4.2.5.1 Responsibilities include:

- Providing validation oversight guidance
- Providing direction to CCTLs
- Developing and presenting material for IT security training
- Working effectively with international organizations/partners
- Working effectively with commercial IT security vendors and consultants
- Providing IT security advice and guidance to clients
- Serving as a CCTL liaison
- Serving as an NVLAP liaison

4.2.5.2 Minimum Qualifications:

The members of the Technical Oversight Team must possess a Bachelor's degree in computer science, information systems, computer/electrical engineering, or mathematics, or equivalent knowledge acquired through relevant work experience. Team members are required to have comprehensive knowledge of IT security evaluation or certification principles, and possess extensive experience (at least two years) in the CC and/or CEM, acquired by direct involvement with the development and/or application of the CC and/or the CEM.

[CCRA C.4]

4.2.6 Validation Body

Each individual performing validation activities will be designated as a validator trainee, lead validator, or senior validator. Validators progress through each validator designation as their experience and proficiency in performing CC validations improves and as they are approved by NIAP Management.

4.2.6.1 Responsibilities include:

- Performing validation oversight reviews
- Providing direction to CCTLs
- Mentoring new validators and evaluators
- Performing assurance continuity activities
- Performing CC interpretations
- Serving as a CCTL liaison
- Serving as an NVLAP liaison

4.2.6.2 Minimum Qualifications:

The members of the Validation Body must possess a Bachelor's degree in computer science, information systems, computer/electrical engineering, mathematics, or

equivalent knowledge acquired through relevant work experience. The members are required to have comprehensive knowledge of theories and principles of IT security, and possess experience (at least two years) in performing IT security evaluations, CC and/or applying the CEM acquired by direct involvement with the development and/or application of the CC and/or the CEM.

[CCRA C.4]

4.2.7 Business Manager

The NIAP Business Manager will interface with the NSA budget and procurement offices to ensure that NIAP budgeting and finance needs are met.

4.2.7.1 Responsibilities include:

- Submitting the NIAP annual financial plan
- Processing Invoices for payment
- Submitting purchase requirements
- Coordinating with the NIAP Director, on financial matters
- Coordinating with the Contracts Manager on contract matters

4.2.7.2 Minimum Qualifications:

The Business Manager should possess a Bachelor's degree in business finance, business management/administration, or equivalent knowledge acquired through relevant work experience. The Business Manager requires extensive knowledge and experience in the field of financial management, budgeting and contracting, and preferred approaches to interfacing with procurement organizations to facilitate compliance with fiscal requirements.

4.2.8 Contracts Manager

The role and responsibilities of the NIAP Contracts Manager are described in detail in section 4.4 of this manual.

4.2.8.1 Responsibilities include:

- Converting NIAP outsourcing requirements into Statements of Work
- Developing Technical Task Orders for NIAP contract support
- Participating in the acquisition process to acquire NIAP contractor support
- Monitoring and reporting on contractor performance
- Managing NIAP contract requirements
- Acquiring and maintaining a Contracting Officer Representative credential
- Coordinating with the NIAP Director, NIAP Deputy Director, and the Business Manager on contract matters

4.2.8.2 Minimum Qualifications:

The Contracts Manager should possess a Bachelor's degree in business management/administration or equivalent knowledge acquired through relevant work

experience. The Contracts Manager must be experienced with contract development and management, and is required to obtain Contracting Officer's Representative status.

4.2.9 Data/Records Manager

The Data/Records Manager will apply NIAP data/records management procedures in accordance with applicable guidance. This also includes applying NIAP policies and procedures for issuing and managing CC certificates over the lifecycle of a NIAP validated product.

4.2.9.1 Responsibilities include:

- Certificate Management
    - Issuing CC certificates
    - Recognizing CCRA partner certificates
    - Maintaining a Product Compliant List
    - Monitoring certificate use
    - Revoking CC certificates
    - Maintaining certificates over the lifecycle of the product
- Document control

  Overseeing:
    - Approval of NIAP data and documents
    - Distribution of NIAP data and documents
    - Procedures for maintaining NIAP data and documents
- Records Management
    - Maintaining procedures for:
    - Creating NIAP documents
    - Storing NIAP records
    - Accessing NIAP records
    - Auditing NIAP records
    - Archiving NIAP records
    - Disposing of NIAP records

4.2.9.2 Minimum Qualifications:

The Data/Records Manager must be knowledgeable of applicable organization, policies, and procedures governing document control and records management.

4.3 Training

The NIAP Director is responsible for making decisions regarding education and training requirements for staff members. The NIAP Director is also responsible for developing and reviewing individual training plans annually of each staff member. The NIAP Technical Lead may assume these responsibilities.

The NIAP Director should complete the following activities for training:

1. Specify and approve minimum training requirements for functional roles

2. Under member supervision the director will approve or review the individuals training plan and experience profile.
3. Review and update training plans with staff members for whom they are responsible
4. Submit requests to have training plans placed under document control
5. Monitor the implementation of the training plans

4.4 Contracts

NIAP is responsible for all technical decisions and work performed by or on behalf of the NIAP. Any contract or other agreement entered into between the NIAP and any person or organization will be documented to include the arrangements of the agreement, including adherence to NIAP policies and procedures.

[CCRA Article 12, C.4]

4.4.1 Contracts Management

When NIAP determines a need to outsource work, it will perform an assessment of potential contractors and establish a contract or working agreement with them. The NIAP Contracts Manager is responsible for all contracts, working agreements, and assessments of contractors

NOTE: Organizations performing work for the NIAP through contracts or working agreements are all referred to as contractors).

Contracted services will be acquired through appropriate NSA organizations. The NIAP Contracts Manager will ensure NIAP acquisition policies and contracting needs are met and processed through appropriate NSA organizations.

4.4.2 Contractor Selection Criteria

Contractors will be selected based on approved acquisition criteria and their ability to satisfy NIAP needs. Criteria to be used in selecting a contractor includes, but is not limited to:

- Conflict of Interest
- Evaluation experience
- CC and CEM experience
- Technical skills
- Quality Systems Experience
- Available resources

4.4.3 Contractor Assessment and Monitoring

All contractors are required to meet NIAP quality system requirements. Contracts shall conform to NIAP standard operating procedures while performing NIAP work to ensure the quality system requirements.

The activities NIAP may perform in monitoring a contractor depend on the details of the contract or working agreement and may include review of the following:

- Status reports
- Deliverables
- Contractor audit reports

4.5 Resource Management Records

This section lists the records required to support the traceability and integrity of the Resource Management procedures. These records may include the following:

4.5.1 Recruitment and Hiring Records

- Requirements for candidate positions
- Candidate rankings
- Notification of selection letter
- Non-disclosure agreement
- Conflict-of-interest forms

4.5.2 Training Records

- Requirements for each role
- Training plans
- Experience profile
- Document control requests

4.5.3 Contractor Management Records

- Contract or working agreement
- Conflict-of-interest forms
- Contractor solicitation statement (which should include purpose, criteria, etc.)
- Contractor agreement to comply with NIAP standard operating procedures
- Contractor list
- Contractor deliverables (e.g., status report, audit reports)
- Non-Disclosure Agreements

5 Data/Records Management

5.1 Records Management

A record is defined as a document furnishing objective evidence of activities performed or results achieved. NIAP maintains a record system for creating and storing records to demonstrate validation procedures have been effectively fulfilled; particularly with respect to application forms, evaluation reports, surveillance activities, and other NIAP internal documents relating to granting, maintaining, extending, or withdrawing validation. NIAP also maintains records on CCTL accreditation and approval as well as records on internal NIAP quality activities (e.g., audit reports and management reviews). NIAP has established a set of procedures for working with the record system. These procedures apply to both paper and electronic records and are described in the following paragraphs.

[CCRA C.6]

5.1.1 Responsibility for Records

- The NIAP Director is responsible for ensuring all records are managed in conformance with Section 2.2.1.3, NIAP Records Management Policy, and with the procedures identified in this section. Each Functional Manager is responsible for ensuring staff members maintain records documenting the activities associated with their respective function.

- Each staff member that creates a record is responsible for ensuring the record is correctly identified (identification of the record is a function of the type of record); that the record is complete, legible, and dated; that all required signatures and initials are filled; and that the record content is clear, correct, and has not been improperly altered. If a record is proprietary, it must state it clearly.

[CCRA C.6]

5.1.2 Types of Records

Records will be generated and updated for activities performed by each of the functional organizations in NIAP. Folders, consisting of groups of records pertaining to a particular subject, will, at a minimum, be maintained for each product evaluation, CCTL, person employed by the NIAP, and each subcontract or agreement. Folders will be maintained on other subjects at the discretion of the NIAP Director. Copies of records may be stored in multiple record folders when it is relevant and useful. The types of records generated by each NIAP function are described below.

- Quality records are organized by quality function and provide objective evidence of the extent of fulfillment of the requirements for quality or the effectiveness of the operation. They include management review reports, corrective and preventive action records, internal audit records, subcontractor reviews, complaints, disputes, appeals, and results of arbitration.

- Resource records are organized by employee name and include hiring information, qualifications, training history, assignments and performance assessments related to NIAP activities. All resource records follow the NSA records management rules and procedures to ensure there is no violation of privacy.

- Technical Oversight records are organized by evaluation and include all evaluation and validation documentation. This includes all read-ahead submissions, correspondence regarding acceptance or rejection of the evaluation, plans for the evaluation including schedule and validators assigned, status reports, observation reports, audit reports, ETRs, minutes of meetings and reviews, final validation reports, validation decisions, and any other correspondence regarding the evaluations.

- Data Management records include document approvals, document distribution, document change notification, information archiving, information disposal, and proprietary or controlled records access.

- CCTL Administration records are organized by CCTLs and include information and correspondence regarding applications, changing scope of accreditations, renewing accreditations or approvals, withdrawal or suspension of accreditations or approvals, CCTL audits, customer complaints and validator observations.

- Certificate Maintenance records are organized by evaluation and include information about certificate issues and delivery, certificate revocations, certificate maintenance activities, and surveillance activities.

5.1.3 Record Storage and Access

- Each employee is given access to folders of records at the discretion of the functional manager responsible for the folder. The decision for granting access is based on the employee's job requirements.

- All records containing information of a confidential, sensitive, or proprietary nature must not be left on desks unattended, must be locked in office file cabinets when not in use, and must not be given to persons who have not been approved to view the data. Functional managers are responsible for checking work areas on a daily basis to assure sensitive information is not left in the work areas unattended.

- The Records Manager will control access to records based on access control lists established by functional managers and approved by the NIAP Director.

- A folder containing records about a validation or CCTL must be signed out through the Records Manager when the folder is removed from its designated location.

- The server is configured to prohibit unauthorized access to electronic folders. Access permissions are set by the Records Manager based on access control lists established by the functional managers and approved by the NIAP Director.

- The Records Manager will perform backups of electronic records and folders on a scheduled basis.

[CCRA C.10]

5.1.4 Archiving

All records pertaining to an evaluation must be kept for a minimum of five years after the completion of the validation. This includes all records and other papers produced in connection with each validation. Other NIAP records will also be archived and retained for five years. The Records Manager is responsible for archiving information and for creating a record identifying the information being archived and the location of the archive.

[CCRA C.6]

5.1.5 Disposal

- The Records Manager is responsible for proper disposal of information once approval has been obtained from the NIAP Director, and for creating a record of the disposal activity.

- All records supporting an evaluation will be destroyed after the archive period has expired.

- Paper records will be shredded or disposed of in burn bags. Electronic records will be erased using a utility that conclusively overwrites the information.

5.1.6 Retention of E-mail Messages and other Electronic Submissions

- Persons receiving E-mail messages or facsimiles containing substantive information necessary to adequately and properly document the activities and functions of the NIAP must file the message with other records that apply to the same subject.

- Website pages at www.niap-ccevs.org/ containing substantive information necessary to adequately and properly document the activities and function of the NIAP must be saved and filed with other records that apply to the same subject.

5.1.7 Records Management

To ensure the traceability and integrity of the Records Management functions, the following events will be documented and stored as official NIAP records:

- NIAP personnel access to proprietary information and records (date, who had access, what information or records were accessed) is granted on a need-to-know basis.

- Written consent for disclosure of proprietary or sensitive information and records to a third party (date, why disclosure is necessary, NIAP person granting the approval, third party consent)

- Disposal of information or records (date, who authorized the disposal, identity of information or records)

- Movement of information or records to archive (date, who authorized the move, identity of information or records)

5.2 Document Control

NIAP maintains procedures to control documents and data related to the NIAP. This includes documents and data developed by NIAP personnel to implement the NIAP as well as documents and data supplied by CCTLs, sponsors, developers, and subcontractors. The procedures established for document control are document approval, document distribution, document maintenance, and document listing.

[CCRA C.5b]

NIAP should use standard document control identifiers for all documents and data. These standard identifiers should include:

- A document number: a unique number assigned by the NIAP to each publication or form

- A title: each document should have a unique descriptive title

- An author: each publication should be assigned an author or editor

- A publication date: each publication should be given an initial publication date. Effective dates should be included where they are relevant.

- Revision dates: subsequent revisions are numbered and recorded

- Document addendums and/or page change addendums

- A sensitivity marking: all documents not intended for public distribution must be marked to include the restrictions on its distribution (e.g., For Official Use Only)

[CCRA C.5b]

5.2.1 Document Approval

Though the NIAP Director is ultimately responsible for the technical and editorial quality of all documents and data prepared by NIAP personnel, the Functional Managers and Quality Manager are directly responsible for ensuring quality in NIAP documents and data.

5.2.1.1 NIAP Director Document Approval Responsibilities

- Approve all documents and data published for external distribution

- Ensure all documents and data published for external distribution are submitted to the Records/Data Manager with instructions for distribution

5.2.1.2 Functional Managers' Document Approval Responsibilities

- Identify the need for a document or data and obtain the necessary resources to create the document/data

- Review and approve documents and data that are specific to their assigned functional area

- Ensure documents and data are:
  - Appropriately marked with the appropriate document control identifiers (e.g., proprietary, draft, etc.) obtained from the Records/Data Manager
  - Free of routine errors
  - Reviewed and receive approval from the appropriate levels of authority prior to distribution
  - Submitted to the Records/Data Manager for preservation

5.2.2 The Quality Manager's Document Approval Responsibilities

- Ensure quality system documents and data are reviewed and approved.

- Obtain appropriate approval signatures for quality system documentation.

- Ensure quality system documents and data have document control identifiers obtained from the Records/Data Manager and are assigned to the appropriate individual or functional area.

- Ensure quality system documents and data are submitted to the Records/Data Manager along with a distribution list for record control.

5.2.3 Document Distribution

- Documents and data should be distributed according to the NIAP Information Security Policy. The mechanisms for distribution are included in Annex D, or delivered to a NIAP participant by hand.

- To receive notification of documentation updates, the requestor must be on the document or appropriate NIAP distribution list.

- When NIAP receives a request for a document, the Records/Data Manager will determine if the requestor is authorized to receive the document. If authorized, the relevant documents and data will be provided by the Records/Data Manager. If

necessary, a record documenting the delivery of the documents and/or data will be generated.

- Employees, subcontractors, and other persons performing work for NIAP may request documents or data from the Records/Data Manager or may download them from the NIAP web site. The corresponding Functional Manager must approve any requests for NIAP documents and data not releasable to the general public. Any distribution of controlled documents and data must be recorded.

- All public requests for documents and data via mail or phone will be forwarded to the Records/Data Manager for processing. The Records/Data Manager will keep a record of the request as well as a record of the information disseminated and the person or organization to which it was delivered.

[CCRA C,5a, d]

5.2.4 Document Maintenance

Changes to documents and data may occur as the result of a quality audit or review or at the request of any NIAP employee. If the document or data to be revised or issued is externally generated, the NIAP employee should contact the generating organization and coordinate the acquisition of the new/revised document or data.

If the request is for a revision to Quality System documentation or data, the employee should contact the NIAP Quality Manager. If the request is for the addition or revision of other NIAP documents or data, the employee should contact the appropriate Functional Manager.

The Quality Manager and Functional Managers should adhere to the following procedures while maintaining documents and data:

- Documents and data should be updated as necessary to reflect the requested change(s). The Quality Manager and Functional Managers will determine if the change(s) in documentation are required and should obtain the necessary resources to perform the change(s). An updated document should require the same review and approval as a new document. See the Document Approval section above for more information.

- The Records/Data Manager should notify and distribute the updated documents or data once finalized.

- Announcements of new or updated documents and data should be posted to the NIAP web site (see reference Annex D). This information should be posted within five days of approval of the new or updated documents.

- Documents and data that are obsolete or have been superseded by a new document should be removed from the document list and the obsolete or superseded documents or data should not be distributed by the NIAP.

[CCRA C.5]

5.2.5 Document Listings

NIAP will maintain a listing of all documents and data it currently supports. NIAP will maintain a historical record of all documents issued and will archive versions of older documents that are no longer used. This archive will be maintained for 5 years.

The documents and the NIAP web site will be updated by the Records/Data Manager within three days after a new or updated document is issued.
[CCRA C.5]

5.2.6 Document Control Records

The following records are required to support the traceability and integrity of Document Control procedures:

- Requests to Records/Data Manager to list a document or data
- Request to be added or removed from a distribution list
- Requests to receive documents and data
- Document or data transmittal forms
- Document or data change requests

5.3 Certificate Management

NIAP issues CC certificates for products that meet the NIAP CCEVS evaluation criteria. A product that has received a CC certificate is referred to as a validated product. Once a certificate has been issued, NIAP publishes a summary of the certificate information in the Product Compliant List (PCL) and promotes the integrity of CC certificates.

5.3.1 Issuing a CC Certificate

CC certificates are issued to product developers or sponsors on behalf of IT products evaluated and validated against the CC according to established NIAP rules. Valid certificates must be signed by designated NSA signatories. Certificates are valid only for the specific version and release of the product or the particular version of the PP identified on the certificate.

5.3.1.1 Certificate Issuing Procedure

1. Following the decision by the NIAP Director to issue a CC certificate for a product, the certificate is prepared and forwarded to the NSA signatories for signature. The contents of a CC certificate are described in Publication #1, *Organization, Management, and Concept of Operations*.

2. The CCRA partners are notified of the certificate issue through inclusion of the certified product on the Common Criteria Portal Certified Product List (CPL).

3. Records are generated documenting the issuance of the certificate.

[CCRA Article 5, 7]

5.3.2 Recognition of CC Certificates Issued by CCRA Partners

By signing the CCRA, the United States recognizes evaluations performed by other nations within the CCRA, unless stated otherwise. The following procedures are implemented to address problems or issues with CCRA certificates.

5.3.2.1 Procedures for Recognition of CC Certificates Issued by CCRA Partners

- If the NIAP concurs with the CCRA partner's issued certificate, no action is taken.
- If NIAP decides not to recognize the certificate after reading the report, a recommendation is submitted to NSA signatories for final approval.
- If the NSA signatories decide the certificate will not be recognized, NIAP will send a letter to the submitting CCRA partner stating the certificate will not be recognized, along with rational for why the certificate was not recognized.
- CCRA partners are afforded the opportunity to request their product to be placed on the NIAP's Product Compliant List as long as the following criteria are met:

    - Product claimed exact compliance against a NIAP-Approved Protection Profile; and
    - All supporting documentation is submitted to NIAP for review and approval

[CCRA Article 5, 7]

5.3.2.2 Procedure for CCRA Partner Requesting Review/Revocation of a NIAP Issued Certificate

- A CCRA partner may submit a request for NIAP to review/revoke a NIAP issued certificate.
- When this information is received from a CCRA partner, the CCEVS will review the issued certification/validation report and Security Target to assess whether the issued certificate clearly meets the requirements of the CC and the CEM and whether the CCEVS concurs with the conclusions reached.

[CCRA Article 5]

5.3.3 Maintaining a Product Compliant List (PCL)

NIAP shall create and maintain a PCL, identifying products evaluated under NIAP and products evaluated against NIAP approved Protection Profiles. The purpose of the PCL is to provide information to the public about available evaluated products and provide a source of reference for users to verify the current status of issued certificates.

NOTE: Only products meeting NIAP Approved Protection Profiles in accordance with Policy Letter #12, "Acceptance Requirements of a product for NIAP Evaluation", will be placed on the PCL.

For each product on the NIAP PCL that has been successfully evaluated, NIAP shall publish a copy of the certificate, the Security Target, the Assurance Activity Report (AAR), Administrative Guidance, and the Validation Report.

5.3.3.1 Procedure for Maintaining the Product Compliant List

- The NIAP staff member designated to be responsible for maintaining the PCL will establish an entry that includes the certificate information and Validation Report upon receiving information regarding a newly issued CC certificate.
- In the event that the certificate has been issued as part of the NIAP Assurance Continuity Program, the entry should be appended to the already existing entry documenting the issuing of the certificate for an earlier version of the same product. A record of the updated action should be generated.
- Upon receiving notice of a certificate revocation, the maintainer of the Product Compliant List should remove all summary information about the product from the PCL and annotate the entry to note revocation of the certificate and effective date.

[CCRA B.2h, C.11]

5.3.4 Certificate Use Monitoring

NIAP may monitor the use of Common Criteria certificates for each NIAP validated product to verify suppliers adhere to the rules associated with the use of CC certificates. A certificate holder can use the certificate for any purpose as long as such use does not misrepresent or violate the intent or rules of the NIAP or the CCRA. NIAP certificate rules are as follows:

NIAP Validation Certificate holders must:

- Make claims regarding validation only in accordance with the NIAP guidance given in Publication #5, Annex D.

- Immediately discontinue use of all advertising matter that contains reference to the product when the certificate is revoked.

- Use the certificate only to indicate products evaluated and validated using the CC in accordance with a NIAP approved Protection Profile.

- Not use the CC certificate or Validation Report in a misleading manner

- Follow NIAP guidelines for display of the CC Certification Mark

- Inform NIAP of any changes to an evaluated product

- Keep records of all consumer complaints to NIAP relating to the product's compliance with the CC

- Take appropriate action with respect to those complaints or disputes affecting compliance with the requirements for validation; this includes documenting the actions taken

5.3.4.1 Procedure for Monitoring

NIAP will:

- Respond to complaints from product users or any other source on issues regarding a specific product evaluation by examining examples of the product and product literature in question, communicating with the product developer regarding the issues, and initiating action if warranted.

- Document all complaints and subsequent NIAP actions as official records.

- If the misuse of a certificate has been determined, request the perpetrator correct the misuse. If no correction takes place, proceed with administrative, procedural or legal steps to correct the misuse. NIAP may remove the product from the PCL upon determination of certificate misuse.

- Document all monitoring activity in NIAP official records.

[CCRA C.12, C.14]

5.3.5 Certificate Withdrawal

The NIAP Director may recommend that a CC certificate be withdrawn if NIAP determines the product no longer meets the criteria for which it was validated or if the holder of the certificate violates the conditions for its use. A product developer may also request a withdrawal if the developer no longer wishes to be bound by the responsibilities of a CC Certificate holder. If a certificate is withdrawn, the summary information about the validated product should be removed from the PCL and a notation should be made of the withdrawal and effective date.

5.3.5.1 Withdrawal Procedure for certificates issued by NIAP

1. The NIAP Director will initiate withdrawal of a NIAP-issued CC certificate based on evidence presented by NIAP staff conclusively demonstrating the product no longer meets the criteria for which it was evaluated or the holder of the certificate has violated the conditions for its use.

2. The NIAP Director will inform the certificate holder by official letter of the reasons for the proposed certificate withdrawal and the procedure for appealing the action.

3. If the certificate holder does not appeal the proposed withdrawal or correct the documented problem, the NIAP Director will issue a final written decision 30 calendar days after the date of the withdrawal letter. If the certificate holder appeals the decision, withdrawal action is suspended until the appeal is resolved, using the procedures defined in Section 3.4, Complaints and Appeals.

4. If a certificate holder opts to correct an identified problem, NIAP will verify that the corrective action was appropriate and resolve the problem before withdrawing the certificate. The certificate holder will be given 60 calendar days to correct the identified problem and present the evidence to NIAP. If the problem is not corrected within 60 days, the certificate should be withdrawn.

5. The NIAP Director will notify the certificate holder by official letter of the decision to withdraw the certificate.

6. The NIAP Director will pass the information regarding the withdrawal to the person designated to maintain the PCL so that summary information regarding the product can be removed from the list and the certificate withdrawal status will be recorded.

7. Records will be generated that document all activities connected with the withdrawal of the certificate including correspondence with the product developer and removal of the product from the PCL.

[CCRA C.15]

5.3.6 Certificate Management Records

Listed below are the required documents related to issuing, publicizing, managing or revoking CC certificates.

5.3.6.1 Issuing CC Certificate

- Copy of signed certificate
- Summary of certificate information on PCL
- Record of date of posting to PCL, CPL

5.3.6.2 Recognition of CC Certificate Issued by CCRA Partners

- Signatory approval/disapproval

5.3.6.3 Product Compliant List

- Copy of certificate
- Validation Report
- Security Target or Standard Protection Profile
- Record of certificate revocation, if applicable

5.3.6.4 Certificate Use Monitoring

- Document complaint (see Section 5.3.4, Certificate Use Monitoring)

- NIAP action taken to investigate complaint
- NIAP recommended resolution and response
- Record of removal from PCL, if applicable

5.3.6.5 Certificate Revocation

- Document evidence indicating why the product no longer meets criteria for which it was evaluated or violation for conditions of use
- Letter to certificate holder and receipt for proposed certificate revocation
- Document evidence of corrective action
- Document final decision and return receipt
- Record of removal of product from PCL

6 Common Criteria Testing Laboratory Administration

NIAP is responsible for the oversight of Approved Labs and Test Methods. In this capacity, NIAP grants approval for a candidate CCTL to become an approved CCTL, coordinates with NVLAP to conduct audits, and performs validator observations. The procedures for each of these activities are provided in Publication #4, *Guidance to Common Criteria Testing Laboratories*. An overview of establishing and maintaining test methods, conducting proficiency tests and maintaining CCTL administration records is provided below.

6.1 Establishing and Maintaining Test Methods

In NIAP, a test method is a set of procedures used by CCTLs to evaluate products. Each product technology type has an associated Technical Community (TC), and a baseline Protection Profile. Each product technology type may also have an associated PP-Module, Functional Package, PP-Configuration, and an Extended Package (EP) containing additional requirements. Protection Profiles and the functional requirements associated with them are a test method.

Test methods employed by the NIAP are propagated through the Protection Profiles. NIAP provides an *Approved Test Methods List* identifying the NIAP approved test methods that can be used by CCTLs. Additional test methods may be defined based on consumer requirements, technical viability, or NIAP experience.

[NIST 150-20]

6.1.1 Test Method Development

The NIAP responsibilities for developing new test methods are as follows:

- Develop test method requirements
- Obtain the necessary resources for test method development
- Review and provide comments on draft test methods
- Prototype the test method with groups representative of the target community
- Approve all test methods
- Place approved test methods on the NIAP Approved Test Methods List
- Submit the approved test method to NVLAP for use in accrediting labs

[NIST 150-20]

6.1.2 Test Method Maintenance

NIAP is jointly responsible for maintaining existing test methods along with other CCRA participants. To accomplish this, the NIAP will:

- Work with the CCTLs to determine effectiveness and weaknesses in a test method
- Perform yearly independent reviews of existing test methods
- Assign resources to address test method changes
- Coordinate findings with the other CCRA participants
- Update *Approved Test Methods List*

[NIST 150-20]

6.2 Development and Maintenance of Proficiency Tests

NVLAP has determined one element of accrediting CCTLs is to require CCTLs be tested. The purpose of these tests is to determine how well the candidate CCTL can perform the test methods for which they are seeking accreditation. These tests are referred to as Proficiency Tests (PT).

NIAP is responsible for the development and maintenance of PTs used during NVLAP accreditation. NIAP works with NVLAP to ensure that PTs meet both NIAP approval and NVLAP accreditation requirements.

6.2.1 PT Development

NIAP responsibilities for developing PTs are as follows:

- Develop Proficiency Test requirements.
- Obtain the necessary resources for Proficiency Test development.
- Review and provide comments on Proficiency Test objectives.
- Prototype the Proficiency Test with groups representative of the target community.
- Approve all Proficiency Tests.

6.2.2 PT Maintenance

NIAP is responsible for maintaining existing Proficiency Tests. To accomplish this, NIAP will:

- Monitor changes in test methods for current NVLAP scopes of accreditation. This includes modification of existing test methods or the addition of new test methods.
- Review the results of CCTL tests to determine weaknesses in a particular Proficiency Test

- Observe CCTLs during evaluations (e.g., using a validator, to determine weaknesses in a Proficiency Test)

- Update Proficiency Tests based on the results. All Proficiency Test updates are reviewed and approved by the NIAP Director (or designee).

6.3 CCTL Administration Records

The following records are required to support the traceability and integrity of the CCTL Administration procedures.

6.3.1 Requirements for CCTL Approval Records

- Letter of Intent (from candidate CCTL) to become an accredited CCTL
- Response to candidate CCTL based on review of Letter of Intent
- Notification to NVLAP of a candidate CCTL
- NVLAP items as mandated by Handbooks 150 and 150-20
- Test results from NVLAP accreditation
- Notification letter to candidate CCTL approving or disapproving request to become a NIAP CCTL

6.3.2 Establishing and Maintaining Test Methods Records

- Test method requirements
- Test method description (the actual test method)
- Approved test method list
- Test method prototype results
- Test method audits and reviews

6.3.3 Renewal of Accreditation/Approval Records

- NVLAP confirmation of accreditation renewal
- Change request from CCTL regarding status (this will prompt a change in the Approved Laboratories List,)

6.3.4 Withdrawal of Suspension of Accreditation/Approval Records

- NVLAP letter to CCTL informing them of intent to withdraw or suspend the CCTL
- Letter from CCTL informing NIAP of intent to withdraw
- Response from NIAP related to CCTL intent letter
- Change request from CCTL regarding status (which should cause a change in the Approved Laboratories List,)

6.3.5 Audit Records

- CCTL audit reports from NIAP audit
- CCTL audit reports from CCTL audit
- Notice of change in CCTL status

6.3.6 Development and Maintenance of Proficiency Test Records

- Proficiency Test audits , reviews, and feedback forms

7 Assurance Continuity

A certificate is valid only for a specific version of a product. Since most products evaluated continue to change as the products evolve and are enhanced with new features and capabilities, the Assurance Continuity process, implemented by NIAP, provides a means of establishing confidence the assurance of the product is maintained without always requiring a formal re-evaluation. The main deliverable required during an Assurance Continuity re-evaluation is an Impact Analysis Report (IAR). Detailed procedures for performing Assurance Continuity re-evaluations are described in NIAP Publication #6 - *Assurance Continuity: Guidance for Maintenance and Re-evaluation*.

7.1 Assurance Continuity Records

To ensure the traceability and integrity of the assurance continuity function, the following events will be documented and stored as official NIAP records:

- Confirmation correspondence of receiving the IAR
- Maintenance Concurrence Letter delivered to applicant (date sent and date confirmation received)
- Notice to applicant of reasons for not issuing an Assurance Continuity Maintenance Report (ACMR) based on an evaluation (letter or minutes of meeting discussing the matter)
- ACMR and, if applicable, an updated ST posted on the PCL (who posted information and date)
- Certificate, ST, and Validation Report removed from the PCL (who removed information and date)
- Evaluation Technical Report, if applicable
- IAR

Annex A: References

Current versions of the CC/CEM, Common Criteria for Information Technology Security Evaluation.

Current versions of the NIST Handbook 150, *NVLAP Procedures and General Requirements* and *NVLAP Common Criteria Testing*.

ISO/IEC 17025:2005 (formerly ISO Guide 25) — General Requirements for the Competence of Calibration and Testing Laboratories, 2005.

ISO/IEC 17065:2012 — Requirements for Bodies Certifying Products, Processes, and Services, 2012.

Annex B: Acronyms

CC	Common Criteria
CCMB	Common Criteria Maintenance Board
CEM	Common Evaluation Methodology
CCRA	Common Criteria Recognition Arrangement
CCTL	Common Criteria Testing Laboratory
CICO	Check-In/Check-Out
EP	Extended Package
ETR	Evaluation Technical Report
ISO	International Organization for Standardization
NIAP	National Information Assurance Partnership
MR	Memorandum for Record
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
PCL	Product Compliant List
PP	Protection Profile
PT	Proficiency Test
ST	Security Target
TOE	Target of Evaluation
TC	Technical Community
VID	Validation Identification
VR	Validation Report

Annex C: Glossary

This glossary contains definitions of terms used in the Common Criteria Scheme. These definitions are consistent with the definitions of terms in ISO Guide 2 and are also broadly consistent with the Common Criteria and Common Methodology.

Accreditation Body: An independent organization responsible for assessing the performance of other organizations against a recognized standard, and for formally confirming the status of those that meet the standard.

Agreement Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security: An agreement in which the Parties (i.e., signatories from participating nations) agree to commit themselves, with respect to IT products and protection profiles, to recognize the Common Criteria certificates which have been issued by any one of them in accordance with the terms of the agreement.

Appeal: The process of taking a complaint to a higher level for resolution.

Approved Test Methods List: The list of approved test methods maintained by NIAP defines the scope of accreditation for CCTLs. This scope of accreditation list the types of IT security evaluations that CCTLs will be authorized to conduct using NIAP-approved test methods.

Assurance Maintenance: The process of recognizing that a set of one or more changes made to a validated TOE has not adversely affected assurance in that TOE.

Assurance Maintenance Addendum: A notation, such as on the listing of evaluated products, that serves as an addendum added to the certificate for a validated TOE. The maintenance addendum lists the maintained versions of the TOE.

Impact Analysis Report (IAR): A report which records the analysis of the impact of changes to the validated TOE.

Assurance Continuity Maintenance Process: A program within the Common Criteria Scheme that allows a sponsor to maintain a Common Criteria certificate by providing a means (through specific assurance maintenance requirements) to ensure that a validated TOE will continue to meet its security target as changes are made to the IT product or its environment.

Assurance Continuity Maintenance Report (ACMR): A publicly available report that describes all changes made to the validated TOE that has been accepted under the maintenance process.

Check-In/Check-Out (CICO): The process for NIAP to provide validation oversight and to ensure the technical quality of evaluations. Details regarding the CICO process

and the documentation requirements are contained in NIAP's "Check-In/ Check-Out Guidance" (CICO Guide).

Common Criteria (CC): Common Criteria for Information Technology Security Evaluation, the title of a set of documents describing a particular set of IT security evaluation criteria.

Common Criteria Certificate: A certificate issued by NIAP which confirms that and IT product or protection profile has successfully completed evaluation by an accredited CCTL in conformance with the Common Criteria standard.

Common Criteria Evaluation and Validation Scheme (CCEVS): The program developed to establish an organizational and technical framework to evaluate the trustworthiness of IT products and protection profiles.

Common Criteria Testing Laboratory (CCTL): Within the context of the Common Criteria Evaluation and Validation Scheme, an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by NIAP to conduct Common Criteria-based evaluations.

Common Evaluation Methodology (CEM): Common Methodology for Information Technology Security Evaluation, the title of a technical document which describes a particular set of IT security evaluation methods.

Evaluation Evidence: Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

Evaluation Technical Report: A report giving the details of the findings of an evaluation, submitted by the CCTL to NIAP as the principal basis for the validation report.

Evaluation Work Plan: A document produced by a CCTL detailing the organization, schedule, and planned activities for an IT security evaluation.

Interpretation: Expert technical judgment, when required, regarding the meaning or method of application of any technical aspect of the Common Criteria and/or Common Methodology.

National Voluntary Laboratory Accreditation Program (NVLAP): The U.S. accreditation authority for CCTLs operating within the NIAP Common Criteria Evaluation and Validation Scheme.

National Information Assurance Partnership (NIAP): The partnership that included the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) which established a program to evaluate IT product conformance to international standards. Currently, NIST is responsible for the National Voluntary

Laboratory Accreditation Program (NVLAP) and NSA is responsible for the National Information Assurance Partnership (NIAP).

National Institute of Standards and Technology (NIST): A federal technology agency that works with industry to develop and apply technology, measurements, and standards.

Product Compliant List (PCL): A publicly available listing maintained by NIAP Scheme of every IT product/system that has been issued a Common Criteria certificate by NIAP.

Protection Profile (PP): An implementation independent set of security requirements for a category of IT products that meet specific consumer needs.

Re-evaluation: A process of recognizing that changes made to a validated TOE require independent evaluator activities to be performed in order to establish a new assurance baseline. Re-evaluation seeks to reuse results from a previous evaluation.

Security Target (ST): A specification of the security required (both functionality and assurance) in a Target of Evaluation (TOE), used as a baseline for evaluation under the Common Criteria. The security target specifies the security objectives, the threats to those objectives, and any specific security mechanisms that will be employed.

Target of Evaluation (TOE): A TOE is defined as a set of software, firmware and/or hardware possibly accompanied by guidance.

Technical Decision (TD): As a result of responses, NIAP's Technical Rapid Response Teams (TRRT) may publicly issue a decision on the NIAP website. Previously 'Precedent Decisions,' Technical Decisions offer clarification and interpretations of PP requirements and assurance activities.

Technical Rapid Response Team (TRRT): A panel composed of scheme validators to ensure technical consistency across evaluations and validations performed under NIAP.

Validation: The process carried out by NIAP leading to the issue of a Common Criteria certificate.

Validation Report (VR): A document issued by NIAP and posted on the PCL, which summarizes the results of an evaluation and confirms the overall results.

Annex D: NIAP Contact Information

Public information about the NIAP may be retrieved from the NIAP web site at http://www.niap-ccevs.org or can be requested by phone or mail. Phone inquiries may be made to 410-854-4458. Mail inquiries may be directed to:

NIAP Director
Common Criteria Evaluation & Validation Scheme
9800 Savage Road, Suite 6940
Ft. Meade, Maryland 20755-6940

E-mail lists on the NIAP mail server are available for communicating with (and receiving announcements from) NIAP. The e-mail list names and purpose of each mail list (ML) are described below.

T.1 Current NIAP Mail Lists

niap@niap-ccevs.org	For public to submit questions and comments to NIAP staff For NIAP staff and validators to submit records of validation activities
niap-announcements@niap-ccevs.org	For all NIAP announcements including, but not limited to, TC creation and document publication

ValGrams: ValGrams are e-mail messages sent to validators by the senior validator or NIAP management with important information or reminders concerning validation processes, policies or procedures. ValGrams are the primary mechanism the scheme uses for directly communicating with all validators. ValGrams are typically distributed via the NIAP Validators mail list, and often contain instructions that validators must apply immediately in validations.

Labgrams: LabGrams are e-mail messages sent to CCTLs by NIAP management with important information or reminders concerning validation processes, policies or procedures. LabGrams are the primary mechanism the scheme uses for directly communicating with all CCTLs. LabGrams are typically distributed via the NIAP Lab mailing list and are also posted to www.niap-ccevs.org.