

**DEPARTMENT OF EDUCATION
INFORMATION TECHNOLOGY SECURITY**



**How to Independently Verify and
Validate IT Security Findings**

DRAFT

April 2004

Table of Contents

1. INTRODUCTION..... 5

1.1 Background 5

1.2 Purpose and Goals 5

1.3 Reasons For Conducting IV&V of IT Security Findings 5

1.4 IV&V Independence Requirements 6

1.5 Parties Involved in IV&V 6

1.6 Assumptions 7

1.7 Scope of this Guide 7

 1.7.1 Types of IV&V Work 7

 1.7.2 Internal Versus External IV&V 7

1.8 Structure of this Guide 8

2. ROLES AND RESPONSIBILITIES..... 9

2.1 IV&V Management Committee 9

2.2 IV&V COR..... 9

2.3 Chief Information Officer (CIO)..... 10

2.4 Computer Security Officer (CSO)..... 10

2.5 IV&V Teams—Internal vs. External..... 11

 2.5.1 Internal IV&V Team..... 11

 2.5.2 External IV&V Team..... 11

2.6 IV&V Quality Assurance Team 11

3. IV&V PROCESS 13

3.1 Major Phases of IV&V 13

3.2 Clarification/Preparation 13

 3.2.1 Establish Specific IV&V GOALS 14

 3.2.2 Develop a Plan for IV&V 14

 3.2.3 Prioritize Findings for IV&V Action (Internal vs. External, High and Low Priority) 15

 3.2.4 Establish IV&V Performance Standards 15

 3.2.5 Establish an Internal IV&V Team 16

 3.2.6 Select Independent IV&V Contractor..... 16

3.3 Verification and Validation 16

 3.3.1 Perform IV&V 16

 3.3.2 Manage/Monitor IV&V Process 16

3.4 Documentation 17

3.5 Review and Reporting 17

 3.5.1 Formally Accept IV&V Results..... 18

 3.5.2 Update PIP with IV&V RESULTS 18

 3.5.3 Provide Periodic IV&V Results to Inspector General 18

 3.5.4 On-going Maintenance..... 18

4. IV&V TECHNIQUES 19

4.1 General IV&V Techniques..... 19

4.2	Specific IV&V Techniques	19
4.2.1	IV&V Techniques for Management Controls.....	21
4.2.2	IV&V Techniques for Operational Controls.....	21
4.2.3	IV&V Techniques for Technical Controls.....	22
5.	IV&V REPORTING REQUIREMENTS.....	24
5.1	Reporting Requirements and Standards	24
5.1.1	IV&V Assessment Results.....	24
5.1.2	Supporting Documentation	24
5.2	Final Report/Providing IV&V Report to Management Committee	24
5.3	Management Committee Recommendation	25
5.4	Authorization to Close.....	25
APPENDIX A. GLOSSARY OF TERMS		1
APPENDIX B. LIST OF ACRONYMS		1
APPENDIX C. REFERENCES		1
APPENDIX D. IV&V EVALUATION CRITERIA		1
APPENDIX E. IV&V END OF PHASE SUMMARY REPORT		1

DOCUMENT CONFIGURATION CONTROL

Version	Release Date	Summary of Changes
April 19, 2004		First Draft

Draft

1. INTRODUCTION

1.1 Background

This Independent Verification and Validation (IV&V) Process Guide was developed in accordance with the charter of the Department of Education's IT Security Independent Verification and Validation (IV&V) Management Committee. The purpose of the IT Security Independent Verification and Validation Management Committee is to plan for, develop, implement, and manage the IV&V activities with respect to (i) the integrity of the Department's IT security corrective action plans (CAPs); (ii) the Department's compliance with IT security CAPs; (iii) IV&V policies, standards, and procedures; and (iv) the process for qualifying, establishing, and maintaining the independence of IV&V activities and IV&V contractors.

The intended audience for this guide is the Department's information technology (IT) security professionals responsible for the security of the Department's general support systems and major applications (e.g., computer security officers [CSOs], system security officers [SSOs], and network security officers [NSOs]).

1.2 Purpose and Goals

The purpose of this IV&V guide is to provide a baseline set of repeatable procedures to perform Independent Verification and Validations (IV&V) of remediations of reported IT security findings related to Department of Education information technology systems. This guide does *not* serve as a guideline for IV&V of software development efforts; rather, it is strictly focused on existing IT security findings.

The objective of establishing a standard independent verification and validation (IV&V) methodology is to meet the ongoing security monitoring and verification requirements of NIST 800-37 by: (i) selecting an appropriate set of security controls in the information system to be monitored, and (ii) evaluating the effectiveness of the selected controls using established verification techniques and procedures. IV&V is a critical component of ensuring government information systems are worth of the public trust, and therefore must be implemented according to predefined schedules throughout all phases of the system life cycle.

NOTE: This methodology is not intended to repeat any certification and accreditation (C&A) process that may have already been performed, but the procedures contained herein *can* be used to verify the quality and conformance of C&A processes with industry standards and best practices.

1.3 Reasons For Conducting IV&V of IT Security Findings

Reasons for conducting IV&V of reported IT security findings include the following:

- assuring that remediations to fix security findings have in fact been implemented as reported
- providing a status of all (or selected) reported findings and their remediation status

- assuring that the IT system C&A packages are credible and understandable, and that they have been produced by an effective repeatable process.
- assuring that the it systems' certification packages meet applicable federal and departmental policies, procedures, regulations and standards.
- assuring that the appropriate security functions have been properly implemented into the it systems and that risk is within acceptable levels.

1.4 IV&V Independence Requirements

To ensure that any and all IV&V efforts undertaken by the Department are fully free from any conflict of interest, and meet the highest standards of quality assurance, any IV&V contractor selected to perform IV&V for the Department must meet the following criteria for independence:

IV&V independence is established through four mechanisms: technical independence, managerial independence, financial independence, and contractual independence.

- *Technical independence* requires that IV&V personnel not be involved in any stage of the software development process.
- *Managerial independence* requires that IV&V responsibility be vested in an organization that is separate from the development and program management organizations. The independent selection of the artifacts to be examined and tested, the techniques to be used, the issues to be chosen, and the reporting to be made further affirm this independence.
- *Financial independence* requires that the IV&V budget be vested in an organization independent from the development organization.
- *Contractual independence* requires that the IV&V contract be executed separately from the contract for development.

Classical IV&V independence is achieved when all four parameters exist by vesting the IV&V authority in an organization separate from the development organization. This requires that the IV&V organization establish a close working relationship with the development organization while maintaining an independent role.

1.5 Parties Involved in IV&V

The following parties will play an integral in IV&V (specific roles and responsibilities are described in section 2):

- IV&V Management Committee
- Computer Security Officers
- System Security Officers
- IV&V Contracting Officer Representative
- Internal IV&V Review Team

- IV&V Contractor Review Team
- IT System Personnel

1.6 Assumptions

The following assumptions were followed when preparing this guide:

- This guide will be updated to reflect the baseline IV&V requirements specified in NIST publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems*.
- The current version of this IV&V guide covers only reported IT security findings. Once NIST 800-053A has been issued, the guide will be expanded to cover IV&V procedures to be implemented throughout the system life cycle.
- The Performance Improvement Portal (PIP) is fully functional and populated with all system findings, corrective action plans, and any other documents necessary for IV&V.
- All system findings, from all sources (eg, IG audits, CAPs, memos, tracking databases), will be cross-walked and reconciled, and compiled into one central, up-to-date repository—the PIP.

1.7 Scope of this Guide

The goal of this IV&V Guide is to support information system business owners and the OCIO Director for IA and to provide the department with an in-house, independent capability to objectively review, evaluate, substantiate (or repudiate) reported remediations on IT security findings.

1.7.1 Types of IV&V Work

Types of IV & V work covered by this guide may include, but is not limited to:

- open actions items contained in POC remediation plans that address General Accounting Office and ED Inspector General security findings and recommendations (ie., in audit or inspections reports) or contractor security review findings and recommendations (ie., in risk assessment reports).
- open action items contained in security reviews performed by contractors for various POCs.
- certification and accreditation security documents (ie., in system security plans, contingency plans, continuity of operations plans, security test and evaluation plans, and risk assessments) as part of the certification and accreditation process in ED.
- accreditation decision of the DAA in various POCs.
- other security documentation, as may be required

1.7.2 Internal Versus External IV&V

The procedures in this guide apply to both internal and external IV&V efforts.

1.8 Structure of this Guide

Section 1 provided an introduction to the IV&V Guide. The remainder of the document is as follows:

- Section 2.
- Section 3.
- Section 4.

Draft

2. ROLES AND RESPONSIBILITIES

This chapter outlines the high-level roles and responsibilities of the major players in the IV&V process.

2.1 IV&V Management Committee

The IV&V Management Committee shall have the following duties and responsibilities:

- Be directly responsible for the capture and review of IT security CAPs
- Be directly responsible for the prioritization of the IT security CAP implementation activity and associated schedule
- Be directly responsible for the development and implementation of the IV&V policy, procedures and standards
- Review the scope of the IV&V activity and hold consensus to move forward with such activity
- Review the IV&V deliverables and work products for quality and compliance to applicable policies, standards and laws and IV&V objectives
- Confirm and attest to the completeness of any IV&V task under review
- Review with the IV&V cadre any problems or difficulties the cadre may have encountered and establish corrective action
- Ensure that the Performance Improvement Portal (PIP) is updated with IV&V results
- As necessary, exchange dialog with the Department's Inspector General (IG) staff to obtain feed-back on the IV&V activity

2.2 IV&V COR

The COR is responsible for monitoring the programmatic or technical aspects of a contract (or Task Order) and making recommendations to the Contract Officer (CO) for necessary contract administration actions. The COR is designated by, and works directly for, the CO on all matters dealing with the contract(s) to which the COR is designated.

Specific responsibilities of the COR include the following:

- Ensures receipt of appointment memorandum from CO by no later than seven (7) days from the date of award. Reads, signs and returns one copy of the original memorandum to the CO for inclusion in the official contract file within ten (10) days of receipt of the memorandum.

- Monitors individual contracts to assure a contractor's technical performance is in accordance with the contract.
- Provides technical direction to contractors as necessary and appropriate, depending on the type and terms of the contract. The individual named in the contract as the COR is the sole person (other than the CO) with the authority to provide technical direction.
- Maintains regular written communication with the CO concerning all aspects of contractor performance, including, but not limited to, providing monitoring information, advice, and requests for formal administrative action to the CO in a timely manner. Such communication may be informal, such as by electronic mail, but must be in writing so that a written record is available.
- Reviews and makes timely recommendations to the CO as to the approval, disapproval, or other action to take concerning a contractor's submission of (or failure to submit) payment requests, deliverables, interim or final progress and financial reports, or any other requirements of the contract. Maintains a record/summary of payments to date to ensure that short-term progress is viewed as part of the whole to help monitor payment expenditures against total obligations.
- Immediately reports contractor performance problems to the CO/CS.
- Maintains current COR certification in accordance with program requirements. Details may be found on the OCFO/CPO website on connectED <<http://connected/>>.
- Maintain copy of signed and dated COR appointment memorandum in COR files.
- Ensures that security requirements for contractors are adhered to in accordance with ACS Directive OM:5-101, Contractor Employee Personnel Security Screenings <http://connected1.ed.gov/po/om/executive/print/acs_om_5_101_supplement.doc>.

2.3 Chief Information Officer (CIO)

The CIO is responsible for oversight of the IV&V Management Committee, and for coordinating IV&V reporting Plan of Action and Milestone (POAM) items to the Office of Management and Budget.

2.4 Computer Security Officer (CSO)

The Computer Security Officer is responsible for being the interface between the IV&V Management Committee and the program offices. The CSO also provides oversight to system security officers as they complete POAM action items that will be subject to IV&V.

2.5 IV&V Teams—Internal vs. External

One of the major steps in the IV&V of security findings/remediations is determining whether the IV&V will be done by an internal or an external IV&V team (these terms are described below). The IV&V Management Committee makes the decision as to whether the IV&V will be conducted internally or externally. *In general*, IV&V for security findings related to management and operational controls will be done internally; for technical findings, IV&V will be conducted externally.

Whether the IV&V Team is internal or external, the team is directly responsible for conducting the tests necessary to confirm whether or not the actions stated on the CAP to resolve or mitigate the finding were successfully taken. The IV&V Management Committee will provide the IV&V Team with the scope of the testing, specifically identifying the findings requiring verification and validation. It is likely that at any time there will be multiple IV&V Teams (both internal and external) working on different systems or sets of findings. These teams must coordinate with each other to ensure a successful IV&V process. Additionally, it is essential that the IV&V Teams provide support and information, as necessary, to the IV&V Management Committee.

The IV&V Team will use a variety of testing techniques, including, but not limited to documentation review, interviews, network scans. (Please see Section 4 for additional information on testing techniques.) The IV&V Team will also be responsible for documenting the results of the IV&V tests in the standard reporting format introduced in Section 5 of this document and responding to any questions from the IV&V Management Committee.

2.5.1 Internal IV&V Team

The Internal IV&V Team will be comprised of Department of Education employees with the technical background and understanding necessary to perform verification and validation. To remain in accordance with independence requirements, the Internal IV&V Team will not consist of any employees that have had direct involvement with the system under review. Typically, the Internal IV&V Team will be responsible for conducting IV&V on management and operational controls.

2.5.2 External IV&V Team

The External IV&V Team will be comprised of third party contractor support. Typically, the External IV&V Team will be responsible for conducting IV&V on technical controls. However, at times, the External IV&V Team's scope may also include the verification and validation of management and operational controls.

2.6 IV&V Quality Assurance Team

[NOTE: THIS TEAM ADDED BY CHUCK AND BRIDGET—PLEASE REVIEW CAREFULLY FOR THE TEAM'S ROLES AND RESPONSIBILITIES, AS WELL AS THE TEAM'S COMPOSITION]

The IV&V Quality Assurance Team will be responsible for ensuring that the day-to-day activities are proceeding to established standards and schedules, providing daily, "on-the-ground" guidance to, and management of, the IV&V teams, and for interfacing with the Computer Security Officer. The Quality Assurance Team will be composed of system security

officers and other system security personnel and program office staff, such as system owners and managers.

Draft

3. IV&V PROCESS

The purpose of Independent Verification and Validation (IV&V) is to ensure that Federal information systems are performing in accordance with written specifications, and to ensure that security controls are properly and effectively implemented. To be successful, IV&V must encompass a comprehensive workflow, from identifying what it is that needs to be IV&V'ed, to conducting the actual IV&V process and carefully documenting all results, to reporting back to the IV&V Management Committee the results of the IV&V process, to determining/finalizing whether security controls are properly implemented, and if a system is performing up to written specifications.

3.1 Major Phases of IV&V

IV&V at the Department of Education consists of the following four major phases:

- Clarification/Preparation
- Verification and Validation
- Documentation
- Review and Reporting

These phases, and the major steps involved in each phase, are described in detail below.

Note: IV&V may be conducted during any phase of the system life cycle, and the four phases above should be followed no matter during what phase during which IV&V is conducted. However, during which phase IV&V is conducted can influence the level of effort required.

3.2 Clarification/Preparation

IV&V must start with a clear understanding of what, exactly, is to be verified and validated; what the scheduling and budgetary requirements are; who must be involved in the process; and what resources (eg, documents, software, physical access) must be available to complete the process.

The clarification phase will include, but not be limited to, the following types of activities

- Review of existing security documentation, certification and accreditation packages, findings, corrective action plans, security testing and evaluation plans
- Gathering of all necessary documentation (system security plans, contract documents, risk acceptance letters, etc.)
- Discussions with appropriate system security personnel
- Review of contract language and budget and schedule requirements

- Arrangements, if necessary, to conduct walkthroughs of selected facilities
- Review of system diagrams to understand system boundaries
- Preparation of a workplan, with expected deliverables, objectives, scope of work, planned approach, milestones, etc.

3.2.1 Establish Specific IV&V GOALS

Clear goals for each specific IV&V effort must be established during the clarification phase of the IV&V process. These goals will be provided by the Department of Education, but the IV&V contractor must work closely with the Department to ensure all involved parties have a common understanding of goals, expected outputs, and so forth. Examples of IV&V goals are as follows:

- To ensure that a particular security “finding” remediation has been implemented as stated.
- To validate the effectiveness of certification and accreditation activities
- To provide continuous monitoring and improvement of the security posture of Department of Education information systems.

3.2.2 Develop a Plan for IV&V

An IV&V plan is critical to ensuring not only that IV&V goals are met, but that there is a clear path toward meeting those goals. The IV&V Management Committee will work closely with affected system and computer security personnel, as well as contracting officers, to ensure all parties have a clear understanding of what needs to be accomplished.

3.2.2.1 Budget/Schedule

Before starting any IV&V project, the necessary resources must be secured, and a timeline established. The schedule should include all important milestones, and allow time to arrange for any necessary personal interviews and walkthroughs. When possible, IV&V efforts should be coordinated with any other scheduled security reviews (eg, IG audits, risk assessments) so the efforts do not contradict one another.

Note: IV&V of security findings can occur at any time during the year, during any phase of the system life cycle—there is not “set” or regular schedule (eg, quarterly) for IV&V.

3.2.2.2 Contracting Vehicles

Work with the IV&V Contracting Officer Representative to determine the best contract vehicle for external IV&V (or to see if there is an existing IV&V contract vehicle that may be used).

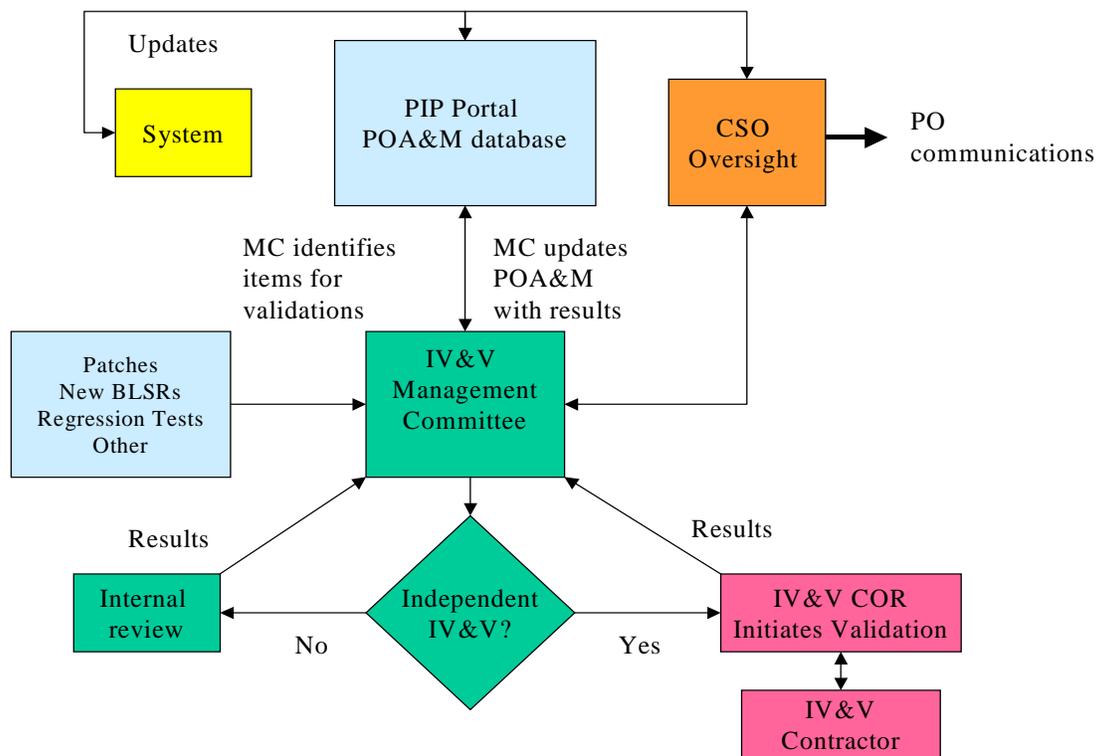
3.2.2.3 Scope of Work

Clarifying the scope of the work is critical to a successful IV&V effort. For IV&V work solely for the purpose of evaluating, verifying, or repudiating reported findings/remediations, each IV&V engagement will be of a narrowly defined scope. The duration of each such IV&V engagement will depend on the number and complexity of the corrective actions to be validated.

For other types of IV&V (eg, IV&V during the system’s development), the scope of work will likely be of a more ongoing nature.

3.2.3 Prioritize Findings for IV&V Action (Internal vs. External, High and Low Priority)

The figure below shows the process to use to determine whether a finding/remediation should be subject to either internal or external IV&V (internal meaning performed by either ED staff or existing contractor staff, or a combination of both; external meaning performed exclusively by a contractor hired specifically for IV&V. In *general*, findings related to management and operational controls will be IV&V’ed internally, while technical findings will be IV&V’ed externally.



Once the decision has been made as to whether the finding/remediation will be subject to internal or external IV&V, each finding/remediation will be prioritized for action. In general, prioritization will be based on the severity of the threat; the nature of the finding (management, operational, or technical); the resources and time required to IV&V the finding; and Federal reporting requirements.

3.2.4 Establish IV&V Performance Standards

This guide serves as the baseline performance standards for IV&V efforts. In addition, any IV&V must meet both Department and relevant Federal IV&V standards. However, situation-specific IV&V projects may require standards above the standards outlined herein. In such cases, these additional standards must be documented in the work plan.

- Note: This document was written before the publication of NIST Special Publication 53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems*. Once this document is published, this guide, as well as IV&V performance standards must be updated to reflect the NIST 53A requirements.

3.2.5 Establish an Internal IV&V Team

Each IV & V team will consist of personnel with sufficient knowledge, skill and competence to perform independent reviews and evaluations of information technology and security programs, processes, and/or systems. Additionally, the IV & V personnel should possess both a theoretical/conceptual grasp of risk, of computer security controls (ie, preventative, detective, corrective controls), of security vulnerabilities, of security weaknesses and of the C-I-A triad (ie., confidentiality-integrity-accuracy). Finally, IV & V personnel should possess a technical and practical understanding of security practices, which includes a working knowledge of automated scanning tools. Accordingly, it is suggested that each IV & V team include personnel with professional certification as CISSP, CISA, CISM or MCSE

3.2.6 Select Independent IV&V Contractor

The IV&V contract officer, with guidance from the IV&V Management Committee, is responsible for soliciting and selecting an IV&V contractor that meets the independence requirements outlined in section 1.4 of this guide. Contract language must establish clear IV&V standards, procedures, and reporting requirements

3.3 Verification and Validation

During the verification phase, the system is examined to ensure that it is performing in accordance with written specifications, and to ensure that reported remediations have been implemented as stated. In some instances, at the direction of the Department of Education, specific security “findings” (noted deficiencies in system security) might be examined discretely, with the express intent of determining if a specific security finding has been sufficiently addressed so that the finding no longer poses an unacceptable security threat. The verification phase will be conducted using either technical or nontechnical activities, or, more likely, a combination of both. These activities are described in more detail in chapter 4 of this guide.

During the validation phase, the results of IV&V activities (reviews, walkthroughs, interviews, technical testing, etc.) are analyzed, and a determination is made as to the status of each particular finding or situation. See chapters 4 and 5 for a detailed description of the activities involved in the validation phase.

3.3.1 Perform IV&V

Before the IV&V contractor begins work the Department must establish criteria for identifying which subset of the security controls in the information system will be evaluated. Note: The criteria established will reflect ED’s priorities and the importance of the information system. The risk level of the information (in accordance with FIPS Publication 199), and the level of the risk itself, also will be considered in any decisions about security control monitoring. All risk levels will be calculated using published ED guidance.

3.3.2 Manage/Monitor IV&V Process

The IV&V Quality Assurance Team will manage the day-to-day operations of the IV&V process. The Quality Assurance Team will also serve as the “front-line” point of contact for the IV&V team, and will be responsible for reporting results, progress, difficulties, etc., up the reporting chain as specified. The team will ensure that reporting formats and schedules are delivered in accordance with the workplan.

3.4 Documentation

A comprehensive IV&V documentation package must be prepared. The package will include the following:

- Final report documenting the procedures and processes used to perform IV&V, the specific issues that were investigated (and their status), recommendations, overall security posture of the IT system, and any unresolved issues. The report will include results for each finding validated, comments regarding any additional information regarding the test objective, test procedure and/or component tested, and findings (if applicable) for each test objective. The findings will be documented in a separate section of the report and will include:
 - Test objective – the BLSR that was verified during IV&V
 - Test objective number – a unique number identifying the test objective
 - Finding description – a description, including how and why, the test objective was not met during testing and what the actual results were when the test procedure(s) were executed;
 - Control tested – management, operational, or technical; and
 - Recommendation – a description of how the finding may be corrected.
- Forms that document the status of existing findings (closed or open), with the appropriate signatures
- Executive-level briefing summarizing the results of the above report.

Specific documentation requirements are contained in chapter 5 of this document.

3.5 Review and Reporting

After IV&V has been completed and the contractor has prepared all documentation according to the requirements in chapter 5 of this document, the IV&V results must be reviewed and approved. This approval consists of a tiered process that is ongoing, starting at the “ground level” (that is, the Quality Assurance Team’s continuous monitoring), then working its way up to the IV&V Management Committee. The IV&V Management Committee will work closely with the appropriate system security personnel and contracting officials to facilitate the review process, and will provide the final, official review and approve of the IV&V effort, and report the results to the appropriate officials.

The following individuals and/or teams will be responsible for reviewing the results of the IV&V effort:

- IV&V Team. The IV&V team itself, whether internal or external, is expected to continually self-assess its efforts. This self-assessment need not be formalized.
- IV&V Quality Assurance Team. The Quality Assurance Team is responsible for assessing and reviewing the deliverables of the IV&V team before they are passed on the COR or IV&V Management Committee. These deliverables will be specified in the IV&V workplan.
- COR Review (External IV&V Only). The COR is responsible for ensuring the timely and correct completion of deliverables. The COR most likely will not review specific deliverables in detail, but will rather consult with the IV&V Management Committee and the Quality Assurance Team as necessary.
- IV&V Management Committee Review. The IV&V Management Committee, based on recommendations from the IV&V Quality Assurance Team, makes the final determination as to the acceptability of the IV&V results.

3.5.1 Formally Accept IV&V Results

After the IV&V results have gone through the reviews described above, the IV&V Management Committee will review and provide formal acceptance of such results (or, conversely, the IV&V Management Committee may reject the results and send the results back the IV&V team to correct).

3.5.2 Update PIP with IV&V RESULTS

After the IV&V results have passed all levels of approval, the IV&V Management Committee will ensure that the IV&V results are entered in the Performance Improvement Portal (PIP).

3.5.3 Provide Periodic IV&V Results to Inspector General

If desired, or required, the Office of the Chief Information Officer will be responsible for providing IV&V reports to the Department Inspector General, in a standard, agreed-upon format.

3.5.4 On-going Maintenance

4. IV&V TECHNIQUES

4.1 General IV&V Techniques

Both technical and non-technical evaluation methods should be used to test and verify a representative sample of the security requirements formulated for each activity. Non-technical evaluation methods lend themselves to aid in the review of security program processes and are used to IV&V most C&A phases. Technical evaluation methods are most suitable for verifying how controls have been implemented and should be used to IV&V a representative sample of security requirements that have been previously tested against the system during the Certification Testing phase. It should be noted however, that supplemental testing methods might be needed if the initial IV&V produces insufficient results during each C&A phase. The list below provides a suggested list of technical and non-technical IV&V evaluation methods.

Examples of Technical Evaluation Methods

- Visual inspections and demonstrations
- Observation/walkthroughs
- Vulnerability assessment tools
- Technical controls reviews

Examples of Non-Technical Evaluation Methods

- Documentation Reviews
- Interviews
- Questionnaires/surveys

Note: The extent of IV&V necessary, and the exact steps taken, will depend on the specific nature of the specific finding, and should be customized to the level commensurate with the level of risk to the information system. Nevertheless, there are certain baseline IV&V procedures that must be followed in all situations. These baseline procedures are described below.

4.2 Specific IV&V Techniques

Listed below are the minimum steps that must be completed for *all* findings (the sections that follow provide additional procedures that must be followed for specific types of findings—ie, management, operational, and technical):

- Review the complete C&A package for conformance with applicable Federal and Departmental policies, procedures, regulations and standards (Security Plan, Security Test and Evaluation Results, Risk Assessment, Contingency Plan, Certification Memo, Accreditation Memo, Security Evaluation Report)

- Identify system security requirements that were tested for certification and accreditation.
- Select representative sample of system's security requirements for testing (10% to 20% is adequate). Make sure to include the security requirements found to be vulnerabilities either in the RA, ST&E or SER.
- Coordinate on-site IV&V visits with appropriate component and system personnel.
- Where appropriate, include system testing to ensure controls are implemented at a level commensurate with the size and complexity of the information system.
- Interview appropriate personnel, such as DAAs, SSOs, and COs, to gather relevant information.
- Observe, via hands-on execution, the system to verify security controls such as password complexity rules, warning banners, and password protected screen savers.
- Interview system personnel (e.g., system administrator, and network administrator) to identify information such as how passwords are distributed, how forgotten passwords are handled, and who is authorized to view audit logs.
- Examine system documentation such as rules of behavior, system security plan, and contingency plan.
- Document any outstanding system deficiencies and vulnerabilities as a result of the on-site technical and non-technical testing.
- Document the extent to which the certification and accreditation meets all C&A IV&V requirements by C&A phase. Review any other sources of outstanding findings (eg, Inspector General audit reports, corrective action plans)
- Ensure that all procedures and polices comply with the minimum requirements established in NIST 800-53A.
- Verify that the finding came from the PIP/POAM database, and that it is the most current version of the finding
- Analyze the finding carefully to ensure you completely understand its implications, and to which process or procedure it applies.
- Determine which phase the system is in (eg, Vision, Maintenance, Disposal)
- Review schedule and resources
- Ensure that the SSP provides a current security baseline against to perform testing
- Report to the IV&V Management Committee

- Review system boundaries, system interconnections
- Keep a log of all IV&V actions performed, in an agreed-upon, standardized format.
- Coordinate with the appropriate system personnel to ensure the parameters of the testing are commonly understood by all.
- Official notification **MUST** come from a Department of Education employee. You can deal with contractors to resolve the status of a finding, but only an FSA system security officer or system owner or manager can sign off that a finding has in fact been closed.
- Accreditation decision review
- Prepare final disposition/validation results in the approved, standard reporting format, which includes a description of the processes and procedures used.
- Ensure that all required signatures are on the final report
- Deliver the final IV&V documentation package to the system security officer for that system

4.2.1 IV&V Techniques for Management Controls

- Analyze the finding carefully to ensure you completely understand its implications, and to which process or procedure it applies.
- Tie the finding to a specific document
- Review the document to ensure the finding has been addressed
- Complete the document review form
- Interview system security and system management individuals to ensure that the control is being applied to operations
- Perform a system walkthrough if necessary
- If necessary, review logs, work orders, contract modifications, etc., to provide a paper trail to ensure the reported remediation has been completed.

4.2.2 IV&V Techniques for Operational Controls

- Analyze the finding carefully to ensure you completely understand its implications, and to which process or procedure it applies.
- Tie the finding to a specific document
- Review the document to ensure the finding has been addressed

- Complete the document review form
- Interview system security and system management individuals to ensure that the control is being applied to operations
- Perform a system walkthrough--observe, via hands-on execution, the system to verify security controls such as password complexity rules, warning banners, and password protected screen savers.
- Interview system personnel (e.g., system administrator, and network administrator) to identify information such as how passwords are distributed, how forgotten passwords are handled, and who is authorized to view audit logs.
- If necessary, review logs, work orders, contract modifications, etc., to provide a paper trail to ensure the reported remediation has been completed.

4.2.3 IV&V Techniques for Technical Controls

IV&V technical testing should include the use of vulnerability assessment tools such as the Internet Security Scanner (ISS) toolset. ISS can scan workstations, servers, and databases for security weaknesses. Before any hands-on testing occurs, the IV&V team should coordinate the entire effort with the appropriate systems personnel so that the parameters of the technical testing are fully understood and agreed upon by all parties involved before any testing begins. The IV&V team may also require time to work with systems personnel to collect preparatory data (i.e., IP addresses) to ensure the system being tested has clearly been delineated and fully covered. Some of the suggested items to be discussed in preparation for technical testing include:

- Scope
- Resources needed
- Network and system identification
- Testing activities limitations
- Explanation of tool capabilities
- Schedule

Following are some of the steps that should be taken for testing technical controls:

- Analyze the finding carefully to ensure you completely understand to which *exact* system/subsystem the finding applies. Break it down to the component level if possible.
- Report any problems in understanding the finding the system security officer (SSO will be responsible for resolving any questions)
- For scan results:
 - Duplicate the original scanning software used, to the extent possible
 - Apply human analysis to the scan results—prioritize scan results as either high, medium, or low
 - Report any disagreements with scan prioritization to the system security officer

- Duplicate the operational environment at the time of the original finding, to the extent possible. Check the system's configuration management plan and any network diagrams and hardware/software inventories. If it is not possible to duplicate the original environment, note how any configuration changes could affect IV&V results.
- Develop a system testing and evaluation plan

Draft

5. IV&V REPORTING REQUIREMENTS

5.1 Reporting Requirements and Standards

After the IV&V testing is completed using the appropriate techniques, a formal IV&V Report must be written. In addition, an executive-level briefing of this report also must be provided.

5.1.1 IV&V Assessment Results

The report must include a description of testing techniques used during the IV&V Process, the scope that they encompassed, as well as a listing of all the findings/remediations tested. The IV&V team must develop an assessment of whether the actions taken to address an IT security finding were in fact completed as stated. The IV&V team must also provide detailed descriptions of any discrepancies between the reported and the validated remediation. All IV&V activities and results will be documented in agreed-upon format.

IV & V evidence will be collected and maintained in a permanent file within the PIP Portal available to the ED IG or to GAO upon request. The IV & V evidence standard will be the “prudent man/prudent person” standard. Accordingly, the IV & V team must gather sufficient evidence:

1. To fully support the opinion that the remediation is complete and is in compliance. In such an instance, the team will issue an “in full compliance/fully implemented” IV & V assessment. To be regarded as fully compliant the actual security control must totally and fully remediate the security vulnerability.
2. To identify that the stated remediation is not complete and is not in compliance/not fully implemented. In such an instance, the team will issue a “not in full compliance/not fully implemented” IV & V report.

5.1.2 Supporting Documentation

Supporting documentation must be included in the PIP portal. Supporting documentation can include, but is not limited to:

- Testamentary or verbal interviews
- System documentation and supporting analysis
- Physical observations
- System generated logs
- Scanning reports
- Penetration testing reports
- Screen prints
- Other manual tracking mechanisms related to finding resolution

5.2 Final Report/Providing IV&V Report to Management Committee

After the IV&V Team completes the IV&V Report, the IV&V Team Lead must provide a signature on the Risk Documentation Worksheet. A separate IV&V Response package must be completed for each finding as reported in the PIP Portal to ensure that each finding is evaluated and reported sufficiently. This package is submitted to the Management Committee for review.

5.3 Management Committee Recommendation

The Management Committee must review each IV&V Response package including Risk Documentation Worksheet IV&V assessment and applicable supporting documentation. If the assessment indicates the finding has not been satisfactorily mitigated, it will remain open in the PIP Portal and monitored by the Management Committee and system management. IV&V must be repeated once the system's CSO indicates there is further evidence available to support closing the finding.

If the assessment concludes that the appropriate controls are now in place to resolve the findings weakness, the Management Committee will determine whether they concur. The Management Committee can:

- **Approve:** The IV&V assessment and supporting documentation provide adequate support that the finding may be closed. The Management Committee Chairperson will sign and date this approval on the Risk Documentation Worksheet and submit it to the Chief Information Officer.
- **Defer:** The Management Committee concurs that the finding has been mitigated, but does not believe that there is adequate supporting documentation. The Management Committee will request that the IV&V team supplement the IV&V Report as necessary.
- **Disapprove:** The Management Committee does not concur with the IV&V assessment. The finding will remain open in the PIP Portal and monitored by the Management Committee and system management. IV&V must be repeated once the CSO indicates there is further evidence available to support closing the finding.

5.4 Authorization to Close

All Management Committee-approved Risk Documentation Worksheet will be submitted to the Chief Information Officer (CIO) for final sign-off. Relying on the evidence provided by the IV&V team and Management Committee, the CIO will serve as the official responsible for providing the final authorization to close the finding. The finding will then be closed in the PIP Portal, and the Risk Assessment Worksheet that contains the signatures of the IV&V Team Lead, Management Committee Chairperson and CIO will be added into the portal.

APPENDIX A. GLOSSARY OF TERMS

Draft

APPENDIX B. LIST OF ACRONYMS

Draft

APPENDIX C. REFERENCES

- CSA of 1987** Computer Security Act of 1987.
- Department of Education IT GSS & MA Inventory Procedures**
Department of Education, Information Technology General Support System and Major Application Inventory Procedures
- Department of Education ITSP**
Department of Education, Information Technology Security Policy
- Department of Education ITSPMP**
Department of Education, Information Technology Security Program and Management Plan
- Department of Education IT RA Procedures**
Department of Education, Information Technology Risk Assessment Procedures.
- Department of Education IT SC Procedures**
Department of Education, Information Technology Security Controls Procedures.
- Department of Education IT CMP Procedures**
Department of Education, Information Technology Configuration Management Plan Procedures.
- Department of Education IT CP Procedures**
Department of Education, Information Technology Contingency Plan Procedures.
- Department of Education IT ST&E Procedures**
Department of Education, Information Technology Security Testing & Evaluation Procedures.
- GISRA** FY 2001 Defense Authorization Act (P.L. 106-398), Government Information Security Reform Act (GISRA), October 2000.
- NIST SP 800-12** National Institute of Standards and Technology (NIST), An Introduction to Computer Security: The NIST Handbook.
- NIST SP 800-18** National Institute of Standards and Technology (NIST), Guide for Developing Security Plans for Information Technology Systems, December 1998.
(<http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.Pdf>)

OMB A-130 Office of Management and Budget (OMB) Management of Federal Information Resources, Circular A-130, Appendix III, 28 November 2000. (<http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>)

PDD-63 Presidential Decision Directive (PDD), Critical Infrastructure Protection, 22 May 1998.

Draft

APPENDIX D. IV&V EVALUATION CRITERIA

Adherence to Required Format and Documentation Standards. The required format for a document will be defined by FSA approved formats, developer approved formats and/or special contract-specified formats. Evaluation with respect to this criterion will consider whether: (1) all required paragraphs are included, (2) all paragraphs are in the required order, (3) each paragraph contains the required content, and (4) the product adheres to requirements regarding formatting, figure placement, and other presentation issues.

Compliance with Contractual Requirements. Contractual requirements are cited in the Statement of Work (SOW), Contract Data Requirements List (CDRL), the text of the contract, applicable higher level specifications, and standards and specifications included by reference in the contract. These sources will be used in evaluating against this criterion.

Internal Consistency. Internal consistency means that the document being evaluated does not contradict itself in either content or style. Elements of consistency are: (1) all statements must be compatible, (2) a given term must mean the same thing throughout, (3) a given item or concept must be referred to by the same name or description throughout, and (4) the level of detail and presentation style must be the same throughout.

Understandability. Understandability is a subjective, yet critical, component of quality. It means that: (1) the document is written using generally accepted rules of grammar, capitalization, punctuation, symbols, and notation, (2) non-standard terms, phrases, acronyms, and abbreviations are defined, (3) the material being presented can be interpreted in only one way, and (4) illustrations are adequately explained.

Technical Adequacy. Technical adequacy criterion covers the following: (1) Is the overall approach sound? (2) Does the information in the document violate known facts or principles? (3) Is it consistent with approaches known to be successful on other projects? (4) Is it well researched or based on proven prototypes? (5) Does the document appear well thought out? (6) Does the approach make sense both technically and practically?

Appropriate Degree of Completeness. Completeness means that all constituent parts are present and that each part is addressed in adequate detail. Because quality evaluations are in-process reviews, they look at products with varying degrees of completeness. The evaluator will judge whether the degree of completeness at a particular time is adequate. Sources for making this determination include project schedules, software development plans, statements indicating whether the document is preliminary or final, and common sense regarding the document's place in the overall development project. At every stage, all required paragraph titles should be present. Completeness of paragraph content depends upon when the required information is, or should be, known based upon the product status as discussed above.

Traceability to Indicated Documents. Traceability means that the document in question is in agreement with a predecessor to which it has a hierarchical relationship. Traceability has three elements: (1) the document in question fully implements the applicable stipulations of the predecessor document, (2) all material in the successor has its basis in the predecessor document,

that is, no untraceable material has been introduced, and (3) the two documents do not contradict one another.

Consistency with Indicated Documents. Consistency between documents means that two or more documents that are not hierarchically related are free from contradictions with one another. Elements of consistency are: (1) all statements must be compatible, (2) a given term must mean the same thing in each, and (3) a given item or concept must be referred to by the same name or description in each document.

Feasibility. Feasibility is the degree to which the design stated in a document can be implemented given the state of the art, schedule and resource constraints, available tools and techniques, and other factors affecting the target system development. An additional consideration is that items that are feasible in isolation may not be feasible when taken together.

Appropriate Requirement Analysis, Design, Coding Techniques Used to Prepare Item. Industry accepted software engineering practices, the SOW, and the development agent's software development plan will establish the basis for this assessment. This evaluation criterion is directly related to other criteria (e.g., conformance with contractual requirements) and provides the basis for determining the soundness of the engineering techniques performed during the development effort.

This evaluation criterion has a direct impact upon the criteria of technical adequacy, feasibility, and resource allocation. In cases where a comment questions the appropriateness of requirements or design analysis in one of the above noted criteria, the comment will be directed to one of the three criteria categories above. Objective evidence (e.g., the results of analysis, simulation, or modeling) will be requested to support the final evaluation of the deficiency noted in the comment.

Appropriate Level of Detail. Level of detail is a subjective criterion whose evaluation is based on the intended use of the document. A document can err in either direction: a document that is supposed to provide requirements might be so detailed as to contain design data; a document that is supposed to provide detailed design might be too high-level. Review of the applicable documentation standards and of other documents of the same type will be used to determine whether the level of detail is appropriate.

Adequate Test Coverage of Requirements. This criterion applies to test planning documents. Aspects to be considered are: (1) Is every requirement addressed by at least one test? (2) Have test cases been selected for an "average" situation as well as for "boundary" situations such as minimum and maximum values? (3) Have "stress" cases been selected, such as out-of-bounds values? (4) Have meaningful combinations of inputs been selected?

Adequacy of Planned Tools, Facilities, Procedures, Methods and Resources. This criterion applies to manuals and planning documents. The evaluation will judge as to whether the planned items will be adequate to fulfill their intended purpose.

Appropriate Content for Intended Audience. Each document has an intended audience and must be evaluated according to how well it addresses the needs of that audience. A system user, for example, does not need design details; those same details are critical for software support

personnel. The applicable documentation standard will provide guidance for making this decision. Within the guidance provided by the documentation standard, however, judgment as to whether the material provided is suitable for the intended audience will be made.

Testability of Requirements. A requirement is considered to be testable if an objective, feasible test can be designed to determine whether the requirement is met by the software. The requirements must be standalone and be compared against the expected results from the test. Compound requirements or vague requirements are difficult to test and should be avoided.

Consistency Between Data Definition and Data Use. This criterion applies primarily to design documents. It refers to the fact that the way in which a data element is defined should match the way that it is used in the software logic.

Adequacy of Test Descriptions/Procedures (Test Inputs, Expected Results, Evaluation Criteria). Test cases and test procedures should be sufficiently clear and specific that a person (other than the author of the test case or procedure) could execute the test and judge unambiguously whether the evaluation criteria had been satisfied.

Completeness of Testing. Testing is complete if all test cases and all test procedures have been carried out, and all results have been fully recorded, analyzed and reported.

Adequacy of Retesting. Retesting consists of repeating a subset of the test cases and test procedures after software corrections have been made to correct problems found in previous testing. Retesting is adequate if: (1) all test cases and test procedures that revealed problems in the previous testing have been repeated and the results have met acceptance criteria, and (2) a selected subset of the test cases and test procedures that revealed no problems during the previous testing, but that are needed to evaluate continued correct operation of the modified software, have been repeated and the results have met acceptance criteria. Criterion 1 is straightforward to evaluate. Criterion 2 is subjective. Complete retesting, using all test cases and all test procedures, is not often practical. A judgment will be made as to: (1) are the selected test cases and procedures those most likely to have been affected by the software changes, and (2) are the selected test cases and procedures those whose outcome is most important? These will be the primary criteria for judging the adequacy of retesting.

APPENDIX E. IV&V END OF PHASE SUMMARY REPORT

Draft