OFFICE OF THE INSPECTOR GENERAL
CORPORATION FOR NATIONAL AND
COMMUNITY SERVICE

Review of
The Corporation for National and Community Service's
System Development Life Cycle

OIG Audit Report Number 01-35
December 11, 2000

Prepared by:

KPMG, LLP
2001 M Street, NW
Washington, DC 20036

Under Corporation for National and Community Service
Office of the Inspector General
Purchase Order # 200008020002
General Services Administration Contract # GS-23F-8127H

This report was issued to Corporation management on May 25, 2001. Under the laws and regulations governing audit follow up, the Corporation must make final management decisions on the report's findings and recommendations no later than November 23, 2001, and complete its corrective actions by May 25, 2002. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.

CORPORATION
FOR NATIONAL
SERVICE

Office of Inspector General
Corporation for National and Community Service

Review of the Corporation for National and Community Service's System Development Life Cycle
OIG Audit Report Number 01-35

The Corporation has installed several new computer applications and system upgrades in recent years and continues with plans to develop and install additional major applications and systems. In accordance with our fiscal year 2001 audit plan for review of the Corporation's systems, CNS OIG engaged KPMG, LLP to assess the Corporation's Structured Systems Development Life Cycle (SSDLC) methodology. Their report concludes that the Corporation's methodology provides a good approach to system development, but recommends improvements in three areas - goals of the policy, minimum requirements, and the review of development documents as refinements are made to the system.

CNS OIG participated in the planning of this engagement and reviewed the report, with which we concur, and the work papers supporting its conclusions. We provided copies of the findings and a draft of this report for the Corporation management's review and comment.

In its response to the report (Appendix B), the Corporation agreed with certain of KPMG's recommendations. The Corporation's Chief Information Officer indicated that CNS would incorporate a requirement for a formal test plan and a formal review of CNS systems during their operational life. However, he stated that he does not plan to incorporate detailed guidance as to what those plans and reviews will encompass because the Corporation wanted the guidance to be usable by all Corporation staff for all systems large and small.

Inspector General
1201 New York Avenue, NW
Washington, DC 20525

Review of
The Corporation for National and Community Service's
System Development Life Cycle
Table of Contents

RESULTS IN BRIEF 1

PROJECT OBJECTIVE 3

METHODOLOGY 3

THE CORPORATION FOR NATIONAL AND COMMUNITY SERVICE STRUCTURED SYSTEMS DEVELOPMENT LIFE-CYCLE METHODOLOGY 5

CORPORATION SSDLC METHODOLOGY V. NIST SP 500-153 6

- GENERAL DIFFERENCES 6
- PHASE-BY-PHASE COMPARISON 7
  - *Conceptual Design Phase (SSDLC) v Initiation Phase (NIST)* *8*
  - *Planning Phase (SSDLC) v Definition Phase (NIST)* *9*
  - *Development Phase (SSDLC) v System Design Phase (NIST)* *10*
  - *Implementation Phase (SSDLC) v Programming and Training Phase (NIST)* *11*
  - *Post Implementation and Systems Support Phase (SSDLC) v Evaluation and Acceptance Phase NIST)* *12*
  - *Installation and Operation* *13*

MOMENTUM AND WBRS APPLICATION DEVELOPMENT METHODOLOGY REVIEW 14

SUMMARY OF NOTIFICATION OF FINDINGS 15

APPENDIX A – NOTIFICATION OF FINDINGS A-1

APPENDIX B – CORPORATION RESPONSES TO THE DRAFT B-1

December 11, 2000

Inspector General
Corporation for National and Community Service:

At your request, KPMG, LLP (KPMG) performed a Software Development Life Cycle (SDLC) Review on the Corporation for National Service's (the Corporation) Structured Systems Development Life-Cycle (SSDLC) Methodology. The primary purpose of this review was to:

- Assess the adequacy of policy and procedures over the SSDLC as applied by the Corporation
- Assess how the Corporation's SSDLC methodology compares to the guidance set forth by the National Institute of Standards and Technology (NIST).

Results in Brief

The Corporation's SSDLC methodology provides a good approach to system development, however we found areas where improvement would be beneficial for clarity and efficient execution of the policies. The Corporation developed a SDLC methodology in Fiscal Year 2000. The Policy is called a Structured Systems Development Life Cycle (SSDLC) Plan. Overall, the SSDLC is a sound document. However, it is limited in stated policies and procedures. While the Corporation tries to place fewer requirements in their plan to allow for flexibility, increased structure is needed. KPMG's recommendations include:

- In the Corporation's SSDLC methodology, there is no statement of the goals of the policy, no enforcement mechanism, and no statement of consequences if the policy is not followed.

  We recommend making the existing purpose statement for the SSDLC more specific. State specific policy goals, document enforcement mechanisms, and consequences for not following the policy, and add documentation references for further guidance.

- A stated goal of the Corporation's SSDLC methodology is to provide guidance in producing methodologies specific to the development of applications. This approach is very accommodating, but the policy lacks specific minimum requirements and provides no uniformity to the application development process. The guidance provided is not enough to ensure that the coverage for software development will be adequate. Also, the guidance is vague regarding the process of approving the various

deliverables.

Specifically missing is a requirement for a Risk Analysis, a System Decision Paper, and a formal Test Plan in the Corporation's SSDLC methodology. In addition, the Planning Phase of the SSDLC does not explicitly address the incorporation of controls, audit capabilities, and security measures.

KPMG recommends the issue of insufficient guidance be addressed by providing appropriate references either to internal guidance (e.g., sample formats, output from previous developments) or external documents (e.g., NIST SP 500-153).

Also, require a statement of compliance that describes how the SSDLC will be applied to a specific development. This statement should be brief and concise, perhaps a one or two-page form that provides pre-defined options for each phase and space for comments and rationale for exceptions. This should be reviewed and approved prior to initiating procurement or authorizing an in-house development effort. Accordingly, an approval process for specific SSDLC Methodologies and other deliverables should be established.

A high-level Risk Analysis should be required within the Project Plan prepared during the Conceptual Design Phase.

The Work/Project Plan should address the rationale for selecting the design approach chosen for the application.

The System Design delivered as part of the Planning Phase should explicitly address controls, audit capabilities, and security.

The security and internal controls of every application should be part of the Detailed System Design. A formal Test Plan should be provided along with the tests and test data.

- The Corporation's SSDLC considers that most development documents are complete during the beginning phases of the SSDLC. The SSDLC does not have a requirement to re-visit these documents as refinements are made to the system.

  We recommend an Evaluation and Acceptance Phase, similar to that described in SP 500-153, be added after the Implementation Phase. During this new phase the Detail System Design, the Audit Plan, all manuals and training materials should be reviewed and updated. Just like the Evaluation and Acceptance Phase in the NIST SP 500-153, this new Phase should include an analysis of all test results, a security review, and all necessary sign-offs for the transition to and operation of the new application.

KPMG also found that even though the development of the Momentum and WBRS applications predates the Corporation's SSDLC policy and that the Momentum implementation is based on a commercial-off-the-shelf (COTS) product, the process followed during their development and implementation is consistent with the SSDLC methodology designed by the Corporation.

Project Objective

The objective of this review was to assess the Corporation's SSDLC methodology to determine the adequacy of policy and procedures over the SDLC as applied by the Corporation. In addition, KPMG was to determine, through comparison, how the Corporation's SSDLC compares to the SDLC guidance set forth by the National Institute of Standards and Technology's (NIST) Special Publication (SP) 500-153.

Methodology

In conducting the review, we were guided by the provisions of NIST Special Publication 500-153, *Guide to Auditing for Controls and Security: A System Development Life Cycle Approach* (SP 500-153). Using this publication, we evaluated the Corporation's SSDLC methodology and the way it might have been applied to the development of Momentum and Web Based Reporting System (WBRS) applications. To make that judgment, KPMG requested and reviewed documentation relating to the various phases as described in the Corporation SSDLC. We also examined

- the similarities and differences between SP 500-153 and the Corporation SSDLC;
- the changes in system development approaches since the publication of SP 500-153;
- applicability of both SDLC methodologies; and
- the Corporation's goals.

KPMG considered the fact that the development of both applications predated the Corporation policy regarding the SSDLC. It also noted that Momentum is a COTS package and WBRS was developed by an outside third-party under contract to CNS thereby limiting the Corporation's involvement in the life cycle of the applications.

This report documents a phase-by-phase analysis of the coverage of the Corporation SSDLC. The report also provides a comparison summary, a table indicating the documentation obtained for each phase, observations, and recommendations.

Our procedures were performed in accordance with *Government Auditing Standards* for performance audits as issued by the Comptroller General of the United States.

The Corporation's response to the SDLC review is included in Appendix B. The Corporation referred to the recommendations in this report as useful and agreed to make roles, responsibilities, and expectations more explicit in the SDLC. They will incorporate a requirement for a formal test plan and for a formal review of the system during its operational life. However, they do not plan to provide detailed guidance as to what those plans and reviews will encompass.

The Corporation for National and Community Service Structured Systems Development Life-Cycle Methodology

The Corporation's SSDLC methodology is documented in OIT Policy 378 effective April 27, 2000. It was implemented as a policy. Its stated purpose is to "*describe a structured approach for systems development from systems planning and design through implementation and support.*" This policy describes the methodology as a series of steps that can be followed to build systems faster, at lower cost, and with less risk. Furthermore, the policy mandates that the Corporation will use the policy as a guideline.

The fact that this SSDLC was issued as a "policy" seems to indicate that the Corporation wants to establish a uniform approach to system development. However, the documented expectations are vague. It seems that this process is not to be strictly maintained as long as the general approach of the SSDLC Plan is followed. While this approach is very accommodating, it results in a policy and related procedures that do not address the specifics necessary to adhere to the SSDLC. The policy lacks detail and is not sufficient as stand-alone guidance in developing specific processes. The SSDLC's criteria for declaring a particular methodology compliant or non-compliant are ambiguous. No statements regarding the enforcement mechanism and/or the consequences of not following the policy are made.

The weak areas could be strengthened by adding the following:

- Appropriate documentation references as additional guidance,
- Specific background information to the goals for each phase leaving less to interpretation,
- Minimal requirements for compliance; and
- Statements regarding the consequences for non-compliance.

A policy that does not include appropriate structure may not allow the policy to function as intended. Minimum standards provide consistency and protect the Corporation's interests.

Corporation SSDLC Methodology v. NIST SP 500-153

General Differences

NIST SP 500-153, (*Guide to Auditing for Controls and Security: A System Development Life Cycle Approach)* requires that the System Decision Paper, Audit Plan, Project Plan, User Manual, and Operations/Maintenance Manual be revised in various Phases, while the Corporation's SSDLC considers them complete after the first revision. The practice of continually updating the documentation ensures that all documents represent the product in its current state. It also ensures that, as the development of the application progresses, the end product will be consistent with the stated requirements.

It is recognized that continual documentation efforts could consume a great deal of resources, delay development, implementation, deployment, and complicate the task of maintaining records. The approach in the Corporation's SSDLC may be more practical. However, we recommend that a mechanism for updating these documents be incorporated into the later phases of the Corporation's SSDLC.

The SDLC methodology in SP 500-153 places a greater emphasis on planning, design, and testing than does the Corporation SSDLC. The SP 500-153 also imposes a greater burden on the development process, but early planning clearly helps

- avoid leaving out controls that are costly or impossible to add later,
- improve code quality and robustness, and
- ensure a smoother conversion and deployment.

KPMG recommends that these issues be sufficiently addressed within documents already required by the Corporation, such as the System Specification.

Phase-by-Phase Comparison

The following table provides a side-by-side comparison of the Corporation's SSDLC phases against those in NIST SP 500-153.

The phases of the SSDLC vs. the NIST SDLC are:

	Corporation SSDLC	**NIST SDLC**
Phase 1	Conceptual Design	Initiation
Phase 2	Planning	Definition
Phase 3	Development	System Design
Phase 4	Implementation	Programming and Training
Phase 5	Post Implementation and System Support	Evaluation and Acceptance
Phase 6		Installation and Operation

Each table below is an analysis and comparison of the phases outlined in the Corporation SSDLC and in NIST SP 500-153.

Conceptual Design Phase (SSDLC) v Initiation Phase (NIST)

The Corporation's SSDLC maps rather closely to the NIST SP 500-153 on the initial SSDLC Phases. In the Conceptual Design Phase, Management identifies the need for a system and develops a high-level work plan. SP 500-153 defines the Initiation Phase as identifying and validating the need, exploring alternative functional concepts, evaluating risks and performing cost/benefit analysis.

Corporation SSDLC	NIST SP 500-153
Conceptual Design –Identify the need for a system and develops a high-level work plan. Outputs: Needs Statement; Feasibility/Cost/Benefit Analysis; and High-level Work/Project Plan.	**Initiation** – Identify and validate need, explore alternative functional concepts, evaluate risks and perform cost/benefit analysis. Outputs: Needs Statement; Feasibility Study; Risk Analysis; Cost/Benefit Analysis; and System Decision Paper.

The Conceptual Design Phase merges the Feasibility Study, Risk Analysis, and Cost/Benefit Analysis required by the Initiation Phase (NIST) into a single document and calls for a high-level Work/Project Plan. In the SP 500-153, the Project Plan is part of the second phase. The SP 500-153 also calls for a System Decision Paper that is not required by the Corporation and is presumably incorporated or implied by the Work/Project Plan.

Planning Phase (SSDLC) v Definition Phase (NIST)

In the Planning Phase, system developers and users determine functional, quality, and architecture requirements of the system identified in the conceptual design phase. They also design the system to meet those requirements, and plan for development and implementation. In the Definition Phase (NIST), the participants (participants are not specified) define functional requirements, initiate planning of the system, identify security measure and control requirements, develop a project plan for system development management with goals and activities for all subsequent phases, and develop an Audit Plan.

Corporation SSDLC	NIST SP 500-153
Planning –Determine functional, quality, and architecture requirements of the system identified in the conceptual design phase, design the system to meet those requirements, and plan for development and implementation. Outputs: Requirements Document; Architectural Model; System Specification; Database Design Document; and Migration Strategy.	**Definition** – Define functional requirements, initiate planning of the system, identify security measure and control requirements, develop project plan for system development management with goals and activities for all subsequent phases, develop Audit Plan. Outputs: Audit Plan; Project Plan; Functional Requirements Document; Functional Security and Internal Controls Requirements Document; Data Requirements Document; Data Sensitivity/Criticality Description; and Revised System Decision Paper.

While the Corporation's SSDLC Planning Phase involves system developers and users to chart the process of designing, implementing, and deploying the application, the SP 500-153's Definition Phase does not define the participants and is still performing preliminary steps, and aiming at addressing often ignored or postponed issues like controls, security, and audit. These are important areas to address that are not spelled out in the Corporation SSDLC, but could well be part of the Requirements Document and the System Specification. KPMG recommends that covering these areas be mandatory in the Corporation SSDLC.

Development Phase (SSDLC) v System Design Phase (NIST)

The Development Phase is where the actual code is designed, developed (written), and de-bugged. Training and reference materials are also developed during this phase.

Corporation SSDLC	NIST SP 500-153
Development –Code and test the system designed in the planning phase and prepare for training and implementation Outputs: Detailed System Design; All required code, test data, data conversions, and system tests; and User and Training Manuals.	**System Design** – Produce System /Design, approve security specifications, identify Validation, Verification, and Testing goals, and review and revise Risk Analysis and Project Plan. Outputs: Revised Project Plan; Revised Audit Plan; System/Sub System, Program, and Database Specifications; Security and Internal Control-Related Specifications; Validation, Verification, and Testing Plan and Specifications; and Revised System Decision Paper.

Although the goal of the SSDLC's System Design Phase is similar, it focuses on the design (no actual code is developed) and requires several specialized deliverables plus updates to the Project Plan, Audit, and Decision Paper. The NIST requirements are greater and more specific than those in the Corporation's SSDLC. We recommend that the Corporation's SSDLC require security, audit, and internal controls be part of the Detailed System Design and that a Testing Plan be provided along with the tests and test data.

Implementation Phase (SSDLC) v Programming and Training Phase (NIST)

The Implementation Phase is where the actual application is installed, tested, and accepted. Prior to this Phase, all code is completed and testing has begun. As part of the Implementation Phase, users are trained and enlisted to perform user acceptance testing.

Corporation SSDLC	NIST SP 500-153
Implementation –Learn and test the system to ensure it meets user requirements. If the users accept the system, the system is installed and/or converted to the new system. Outputs: User Acceptance Test; and Implemented/Installed/Tested System.	**Programming and Training** – Produce programs ready for testing, acceptance, and installation, preparation of training, user, and operational manuals, and a preliminary Installation Plan. Outputs: User Manual; Revised Audit Plan; Operations/Maintenance Manual; Revised Project Plan; Validation, Verification, and Testing Plan and Specifications; Installation & Conversion Plan; and Revised System Decision Paper.

The corresponding NIST Phase stays one step behind by focusing at this time on code development, development of reference and training materials, updating the Audit Plan, and the Project Plan. During this phase planning for the tests, the transition, and the conversion is also completed. Some training is also conducted during this phase.

Post Implementation and Systems Support Phase (SSDLC) v Evaluation and Acceptance Phase NIST)

This is the final Phase under the Corporation's SSDLC. Operational policies and procedures are defined and updated during this Phase. All system maintenance, updates and modifications, and assessments (audits/reviews) also take place in recurring fashion during this Phase. These activities all produce output documentation that range from policy statements to code updates.

Corporation SSDLC	NIST SP 500-153
Post Implementation and System Support –Continuously monitor the implemented system to ensure it measures up to the expectations and requirements developed in previous phases and to enhance the system as needed to increase the system's useful life. Outputs: Process and/or policies for monitoring system, tracking modifications, interacting with users, requesting modifications, and maintaining the system; System modifications and updates; and System evaluations and reviews.	**Evaluation and Acceptance** – Conduct integration and acceptance testing, an OMB A-130 review, and produce an approval letter from the responsible accrediting official. Outputs: Revised Audit Plan; Revised Project Plan; Revised User Manual; Revised Operations/Maintenance Manual; Installation & Conversion Plan; Test Analysis & Security Evaluation Report; and Revised System Decision Paper.

KPMG recommends that a requirement for the tracking and maintenance of these documents on an on-going basis be added to this Phase. The corresponding development phase under SP 500-153, the Evaluation and Acceptance Phase, focuses on analyzing tests, completing security evaluation, updating Audit and Project Plans, User Manuals, and Decision Paper. An equivalent is not explicitly defined in the Corporation's SSDLC. We recommend that such a Phase be added either as a stand-alone or as the final part of the Implementation Phase.

Installation and Operation

The NIST SP 500-153 defines this Phase as implementing the approved operational plan, continuing operations, budgeting and controlling all changes to the system throughout its life.

Corporation Structured Systems Development Methodology	NIST Special Pub 500-153
No corresponding phase.	**Installation and Operation** – Implement the approved operational plan, continue operations, budget accordingly, and control all changes to the system throughout its life. Outputs: Revised Audit Plan; Revised Project Plan; Revised User Manual; and Revised Operations/Maintenance Manual.

This phase is more akin to some activities performed during the Post Implementation and Systems Support Phase defined in the Corporation's SSDLC. The deliverables from this Phase, other than the installed, operational, and maintained systems are all updates to documents produced in previous Phases.

Momentum and WBRS Application Development Methodology Review

The methodology followed in the development of the Momentum and WBRS applications was reviewed as part of this Task. The goal was to document the process under the Corporation SSDLC and NIST Special Publication 500-153 to provide a comparison, illustrate strengths and possible weaknesses in the Corporation's SSDLC and/or its application, and make any pertinent recommendations for its improvement.

In this portion of the Systems Development Life Cycle Review, we first compared the Momentum and WBRS application documentation to the Corporation's SSDLC. Secondly, we compared the documentation of both applications to the guidance provided by NIST Special Publication 500-153. It should be noted that the intended scope of the SP 500-153 is to perform an NIST SDLC audit concurrent with the development of an application. However, because the scope of this SDLC review was performed on an existing system, this review focuses on the documentation that was provided in response to the requirements of the methodology.

The Momentum application is a commercial product implemented by the Corporation to replace the old financial package, Federal Success. Momentum went into production in September 1999 and therefore pre-dates the establishment of the Corporation SSDLC's methodology as Corporation policy (effective 4/27/00). It is also important to note that being a commercial product; the Corporation had limited control over the actual development of the software. However, a great deal of documentation was collected showing good coverage of the areas included in the SSDLC.

Aguirre International, a CNS Training and Technical Assistance Provider, developed the WBRS application. The initial WBRS pilots were launched in 1998. According to Corporation Management, by March of 1999 WBRS was in production in all states. This deployment also pre-dates the establishment of the Corporation's SSDLC methodology. Nonetheless, the Office of Information Technology (OIT) was able to either present completed documents or collect information that met the criteria for most SSDLC requirements. Areas where coverage deficiencies were more noticeable include the lack of implementation sign-off documentation and the lack of a documented migration strategy.

We found that significant emphasis was placed on important areas such as the development of manuals, system documentation, and training materials. Considering that Momentum and WBRS were implemented prior to the effective date of the Corporation SSDLC policy, the process followed provides adequate coverage.

Summary of Notification of Findings

A total of three Notification of Findings (NOFs) were issued during the course of the project. The table below contains a synopsis of the findings and the recommendations documented in each NOF located in Appendix A.

Condition	Recommendation
In the Corporation Structured Systems Development Life Cycle (SSDLC) methodology, there is no statement of the goals of the policy, no enforcement mechanism, and no statement of consequences if the policy is not followed.	Make the existing purpose statement for the SSDLC more specific. State specific policy goals, document enforcement mechanisms, and consequences for not following the policy, and add documentation references for further guidance.
A stated goal of the Corporation Structured Systems Development Life Cycle (SSDLC) methodology is to provide guidance in producing methodologies specific to the development of applications. This approach is very accommodating, but the policy lacks specific minimum requirements and provides no uniformity to the application development process. The guidance provided is not enough to ensure that the coverage for software development will be adequate. Also, the guidance is vague regarding the process of approving the various deliverables. Specifically missing is a requirement for a Risk Analysis, a System Decision Paper, and a formal Test Plan in the Corporation's SSDLC. In addition, the Planning Phase of the SSDLC does not explicitly address the incorporation of controls, audit capabilities, and security measures.	The issue of insufficient guidance should be addressed by providing appropriate references either to internal guidance (e.g., sample formats, output from previous developments) or external documents (e.g., NIST SP 500-153). Require a statement of compliance that describes how the SSDLC will be applied to a specific development. This statement should be brief and concise, perhaps a one or two-page form that provides pre-defined options for each phase and space for comments and rationale for exceptions. This should be reviewed and approved prior to initiating procurement or authorizing an in-house development effort. Accordingly, an approval process for specific SSDLC Methodologies and other deliverables should be established. A high-level Risk Analysis should be required within the Project Plan prepared during the Conceptual Design Phase. The Work/Project Plan should address the rationale for selecting the design approach chosen for the application

Condition	Recommendation
	The System Design delivered as part of the Planning Phase should explicitly address controls, audit capabilities, and security. The security and internal controls of every application should be part of the Detailed System Design. A formal Test Plan should be provided along with the tests and test data.
The Corporation's SSDLC considers that most development documents are complete during the beginning phases of the SSDLC. The SSDLC does not have a requirement to re-visit these documents as refinements are made to the system.	An Evaluation and Acceptance Phase, similar to that described in SP 500-153, should be added after the Implementation Phase. During this new phase the Detail System Design, the Audit Plan, all manuals and training materials should be reviewed and updated. Just like the Evaluation and Acceptance Phase in the NIST SP 500-153, this new Phase should include an analysis of all test results, a security review, and all necessary sign-offs for the transition to and operation of the new application.

*****

This report is intended solely for the information and use of the Office of the Inspector General, the management of the Corporation for National and Community Service, and the United States Congress and is not intended to be and should not be used by anyone other than these specified parties.

Felipe Alonso
Partner, KPMG, LLP

Notification of Findings Appendix A

Notification of Finding: Missing statement of the SSDLC policy goals.

Condition:
In the Corporation Structured Software Development Life Cycle (SSDLC) Plan, there is no statement of the goals of the policy, no enforcement mechanism, and no statement of consequences if the policy is not followed.

Criteria:
OMB Circular A-123, Management Accountability and Control

Cause:
Although the more compact approach used in the Corporation's SSDLC provides a more favorable balance between documentation and development effort than the NIST criteria, it lacks some important elements and should be updated. The policy as it stands is unenforceable, no responsibility over its enforcements is assigned, and there are no objective criteria for establishing compliance even if it were to be applied.

Risk:
Failing to indicate policy goals, enforcement mechanism, and consequences for not following a policy will weaken the requirement on all policies and directives. The purpose of a policy should not be to describe an approach; it should be to mandate minimum requirements.

Recommendation:
Make the existing purpose statement for the SSDLC more specific. State specific policy goals, document enforcement mechanisms, and consequences for not following the policy, and add documentation references for further guidance.

Goals of the policy may include the following: Provide uniformity to the systems/application development process, speed the development process, require adherence to standards and best practices, and provide guidance for the on-going maintenance of applications. The remaining "boiler-plate" should clearly state the enforcement mechanism (e.g., all procurement packages will be reviewed and required to include an SSDLC methodology) and the consequences for non-compliance (e.g., procurement packages may not be processed without the required SDLC methodology).

Appendix A

Notification of Findings

Management Response:

This finding was discussed with Corporation Management on December 14, 2000. Comments from Corporation Management will be deferred until the final report is issued. The Corporation's CIO does not agree with this finding.

Appendix A

Notification of Findings

Notification of Finding: The SSDLC is lacking specific minimum requirements and uniformity.

Condition:
A stated goal of the Corporation Structured Software Development Life Cycle (SSDLC) methodology is to provide guidance in producing methodologies specific to the development of applications. This approach is very accommodating, but the policy lacks specific minimum requirements and provides no uniformity to the application development process. The guidance provided is not enough to ensure that the coverage for software development will be adequate. Also, the guidance is vague regarding the process of approving the various deliverables.

Specifically missing is a requirement for a Risk Analysis, a System Decision Paper, and a formal Test Plan in the Corporation's SSDLC. In addition, the Planning Phase of the SSDLC does not explicitly address the incorporation of controls, audit capabilities, and security measures.

Criteria:
NBS Special Publication 500-153, *Guide to Auditing for Controls and Security: A System Development Life Cycle Approach* (SP 500-153).

Cause:
The Corporation System Software Development Life Cycle methodology does not fully conform to the criteria above. Although the more compact approach used in the Corporation's SSDLC provides a more favorable balance between documentation and development effort than the criteria it lacks some important elements and should be updated.

Risk:
Without uniform guidance the goal of uniformity might not be achievable, thus providing no clear reference to decide if a particular methodology complies with the policy or not.

Although a Risk Analysis is no longer a requirement under OMB Circular A-130, the Circular requires that the decision to implement security measures and controls be based on the perceived risks to systems and applications. Without some kind of risk analysis, it may not be possible to justify the use or non-use of a particular security mechanism during a security review. Further, an understanding of the risk environment of a particular

application is necessary to assess the appropriateness and cost-effectiveness of any security measures.

The System Decision Paper, as defined in SP 500-153, discusses several examples of design approaches considered for application development. The Decision Paper highlights the advantages and disadvantages of each approach and supports the selection of the approach chosen. Such a document helps maintain corporate history of the rationale for specific design decisions. The lack of this documentation may complicate later efforts to update the application.

If security concerns, audit capabilities, and application controls are not considered and incorporated into the overall design, they may end up ignored completely or end up retrofitted into the application. This could result in a weaker, cumbersome application that may be more costly to implement and operate in a safe manner. The possible lack of appropriate documentation of security measures and controls could make application security and controls reviews more difficult and disruptive. It could also complicate software updates and increase the possibility that further updates may conflict with existing controls and security mechanisms.

The lack of a comprehensive Test Plan could make the testing and refining of the application more difficult, time consuming, costly, disruptive, and controversial even if an appropriate battery of tests has been defined.

Recommendation:
The issue of insufficient guidance should be addressed by providing appropriate references either to internal guidance (e.g., sample formats, output from previous developments) or external documents (e.g., NBS SP 500-153, GAO Black Book, etc.).

Require a statement of compliance that describes how the SSDLC will be applied to a specific development. This statement should be brief and concise, perhaps a one or two-page form that provides pre-defined options for each phase and space for comments and rationale for exceptions. This should be reviewed and approved prior to initiating procurement or authorizing an in-house development effort. Accordingly, an approval process for specific SSDLC Methodologies and other deliverables should be established.

A high-level Risk Analysis should be required within the Project Plan prepared during the Conceptual Design Phase.

Appendix A

Notification of Findings

The Work/Project Plan should address the rationale for selecting the design approach chosen for the application

The System Design delivered as part of the Planning Phase should explicitly address controls, audit capabilities, and security.

The security and internal controls of every application should be part of the Detailed System Design. A formal Test Plan should be provided along with the tests and test data.

Management Response:

This finding was discussed with Corporation Management on December 14, 2000. Comments from Corporation Management will be deferred until the final report is issued. The Corporation's CIO does not agree with this finding.

Appendix A

Notification of Findings

Notification of Finding: The SSDLC is missing a requirement to re-visit documentation as refinements are made to the system.

Condition:
The Corporation's SSDLC considers that most development documents are complete during the beginning phases of the SSDLC. The SSDLC does not have a requirement to re-visit these documents as refinements are made to the system.

Criteria:
NBS Special Publication 500-153, *Guide to Auditing for Controls and Security: A System Development Life Cycle Approach* (SP 500-153).

Cause:
The Corporation Structured Software Development Life Cycle methodology does not fully conform to the criteria above. Although the more compact approach used in the Corporation's SSDLC provides a more favorable balance between documentation and development effort than the criteria it lacks some important elements and should be updated.

Risk:
The documentation prepared in the early stages of development of an application is likely to depart from what ultimately is implemented. Failure to document the application as it is delivered, not as designed, will complicate any efforts to enhance it, update it, or review it.

Recommendation:
An Evaluation and Acceptance Phase, similar to that described in SP 500-153, should be added after the Implementation Phase. During this new phase the Detail System Design, the Audit Plan, all manuals and training materials should be reviewed and updated. Just like the Evaluation and Acceptance Phase in the SP, this new Phase should include an analysis of all test results, a security review, and all necessary sign-offs for the transition to and operation of the new application.

Notification of Findings

Management Response:

This finding was discussed with Corporation Management on December 14, 2000. Comments from Corporation Management will be deferred until the final report is issued. The Corporation's CIO does not agree with this finding.

CORPORATION
FOR NATIONAL
SERVICE

April 27, 2001

The Honorable Luise Jordan,
Inspector General
Corporation for National and
Community Service

Dear Ms. Jordan:

We have reviewed the draft audit report *Review of the Corporation for National and Community Service's System Development Life Cycle* (OIG Report Number 01-35 dated December 11, 2000). We are pleased that the auditors found that the Corporation's SDLC methodology provides a good approach to system development.

The report contains some useful suggestions for improving the SDLC document, suggestions that we will take. However, we want to point out that the report is based on an aged and obscure standard and, if fully implemented, would create a document much too bureaucratic for an organization of our size and a document much more likely to be ignored. The Corporation will incorporate in its SDLC the useful suggestions in a manner that will maintain the document's readability and its functionality in our context.

Your report cites as the standard for judging our SDLC, NIST SP 500 - 153, by which we assume the auditors meant NSB SP 500 – 153 a Guide to Auditing for Controls and Security: A Systems Development Life Cycle Approach." No one in the Corporation was familiar with that document. We could find no mention of that document in any document on the CIO Council's extensive web site. With some difficulty, we were able to find the 1988 document offered for sale at NIST for $65. Where agencies have been instructed that this is the preferred model for an SDLC, we do not know. We believe there is a reason no one has heard of the NBS document. It reflects the way in which large systems were built in the mid 1980s and it is a singularly unreadable document.

The Corporation drafted its SDLC about a year ago after reviewing about six such documents from other Federal and State entities. Our document was crafted so that it would be very readable for

1201 New York Avenue, NW
Washington, DC 20525
Telephone 202-606-5000

Getting Things Done.
Americorps, National Service
Learn and Serve America
National Senior Corps

our largely non-technical audience. We kept it reasonably generic so that one policy would be equally suited for use with major systems, which we develop only every few years, and with minor systems that we develop more often. We wanted all Corporation staff to be able to, in fact be required to, read the document, understand it, and develop well thought out systems designs.

As suggested in the report, we will make roles, responsibilities, and expectations more explicit in our SDLC. We will incorporate a requirement for a formal test plan and for a formal review of the system during its operational life. But we will not provide detailed guidance as to what those plans and reviews will encompass. As stated earlier, we want this document to serve equally well for systems large and small. And finally, we will not point the readers of our policy toward the almost impenetrable NBS document.

We would like to thank KPMG's staff for their willingness to discuss this work with us during its development.

Sincerely,

David N. Spevacek
Chief Information Officer

cc: Wendy Zenker
Bill Anderson

RECEIVED
APR 27 2001
OFFICE OF THE
INSPECTOR GENERAL

1201 New York Avenue, NW
Washington, DC 20525
Telephone 202-606-5000

Getting Things Done.
Americorps, National Service
Learn and Serve America
National Senior Corps