MASTER COPY

MISTG Memo No. 08 - 2020

BUREAU OF CUSTOMS

Professionalism Integrity Accountability

MEMORANDUM

TO : **ALL DEPUTY COMMISSIONERS**
ALL DISTRICT and SUBPORT COLLECTORS
ALL OTHERS CONCERNED

FROM : **REY LEONARDO B. GUERRERO**
Commissioner AUG 10 2020

BOC-07-01250

SUBJECT : **System Development and Implementation Policy**

DATE : 03 August 2020

Section 2 of CMO No. 04-2019 states that "Systems Development Division (SDD) shall be responsible for business analysis, requirements gathering, and quality management of systems and software that will either be developed or procured by the Bureau. SDD shall develop the System Development Life Cycle (SDLC) that is congruent to developing secure quality robust software solutions quickly for the Bureau."

In view of the foregoing, all acquisition of software or systems development through a third-party must be coordinated and undergo MISTG Quality Assurance and User's Acceptance Testing before it can be allowed to be used by BOC. The source code, system's documentation and User's Manual must be properly turned over to ensure that MISTG can properly support and sustain the said system.

For strict compliance.

MISTG SYSTEM DEVELOPMENT POLICY

PURPOSE

The purpose of this Policy is to standardize software development for all BOC centrally managed mission critical web applications and web services using industry leading practices. These applications and services typically deal with sensitive data and / or HR-, finance-, importer-, broker-, exporter-, consignee-, employee record-, or BOC related data, and due diligence in protecting this data is required. Standardizing the development approach, coding techniques and support for critical systems will ensure their **maintainability**, security, protection against cyber-attacks and accessibility.

SCOPE

This Policy applies to all employees, consultants and / or contractors involved in the development or modification of enterprise-level centrally managed mission critical applications that support Bureau of Customs. If any provision of this Policy is found to be inconsistent with the provisions of a collective agreement, the collective agreement will prevail, unless the Policy provision is required by law, in which case the Policy provision will prevail.

POLICY STATEMENT

Management Information Systems and Technology Group ("MISTG") is responsible for developing, maintaining, and participating in a System Development Life Cycle ("SDLC") for BOC automation projects. All software or systems which runs on production systems must be developed according to the SDLC. At a minimum, this Policy addresses the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; design specification; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for sensitive BOC information.

All enterprise-level centrally managed mission critical applications developed at or for Bureau of Customs must adhere to development standards and procedures documented in the Software Development Policy

MISTG Application Development Standards guide. These standards include coding techniques, testing strategies, documentation requirements and software release processes that align with industry standards and regulatory requirements.

There must be a separation between the production, development, and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, Quality Assurance test staff must not be permitted to have access to production systems.

Responsibility

This Policy is under the jurisdiction of MISTG System Development Division. The interpretation and application of this Policy is the responsibility of the Information Systems Analyst. Final decisions related to this Policy will be made by the Chief, System Development Division, where required.

DEFINITIONS

Application

Computer programs, procedures, rules, source code and associated documentation and data pertaining to the operation of a computer system.

Mission Critical

A system or application whose failure will result in the failure of BOC operational systems.

System Development Life Cycle (SDLC)

A standardized process for planning, creating, testing, and deploying an application.

COMPLIANCE AND REPORTING

All applications are reviewed at predetermined checkpoints of the SDLC by the Information Systems Analyst or their designate. Any deviations are identified, and corrective action is determined prior to the application being released to production. Electronic authorization indicating standards have been met is required before a new or modified application can be released to production.

MISTG always enforces this Policy and the related Standards. Anyone who has reason to suspect a deliberate and / or significant violation of this Policy is encouraged to promptly report it to the MISTG Help Desk. Policy violations that come to the attention of the MISTG Help Desk will be escalated to the Chief, System Development Division. Policy violations will be assessed, and action taken to remediate the violation subject to collective agreements and / or other contractual conditions.

Where Policy violations are considered severe and / or cannot be easily remediated, the incident will be escalated to the Director, MISTG-PSDS for further action. Periodically, the Deputy Commissioner, MISTG will provide to Executive Committee a summary of all policy violations.

Policy owner:	Chief, MISTG - System Development Division
Authorized by:	Deputy Commissioner, MISTG
Created by:	Information Systems Analyst
Approved by:	BOC Executive Committee
Effective date:	August 2020
Next review:	July 2021
Revision history:	V1.2
Related documents:	CMO No. 04-2019 Bureau of Customs Citizen's Charter 2019 MISTG System Development Life Cycle - Draft

MISTG SYSTEM DEVELOPMENT LIFE CYCLE POLICY

Scope and Purpose

This policy defines the development and implementation requirements for Bureau of Customs Information Systems. This policy applies to all employees at Bureau of Customs and other individuals and organizations who work with any form of software or system development under the supervision of Bureau of Customs.

The purpose of this policy is to provide a methodology to help ensure the successful implementation of systems that satisfy Bureau of Customs strategic and business objectives. This documentation provides a mechanism to ensure that executive leadership, functional mangers, and users (where appropriate) sign-off on the requirements and implementation of systems. The process provides visibility of the design, development, and implementation status needed to ensure delivery on time and within budget.

Policy Goals:

Deliver quality systems which meet or exceed client expectations when promised and within cost estimates.

Provide a framework for developing quality systems using an identifiable, measurable, and repeatable process.

Identify and assign the roles and responsibilities of all involved parties, including functional and technical managers, throughout the system development life cycle.

Ensure that system development requirements are well defined and subsequently satisfied.

Policy Objectives:

Establish appropriate levels of management authority to provide timely direction, coordination, control, review, and approval of the system development project.

Document requirements and maintain traceability of those requirements throughout the development and implementation process.

Ensure that projects are developed within the current and planned information technology infrastructure.

Segregation of Environments

Development will be performed in a dedicated network zone, separate from quality assurance and production.

Quality Assurance will be performed in a dedicated network zone separate from production and development.

System Development Life Cycle (SDLC) Phases

Initial Phase

The purposes of the Initiation Phase are to:

Identify and validate an opportunity to improve business accomplishments or a deficiency related to a business need

Identify significant assumptions and constraints on solutions

Recommend the exploration of alternative concepts and methods to satisfy the need

Feasibility Phase

The Feasibility Phase is the initial investigation or brief study of the problem to determine whether the systems project should be pursued. A feasibility study establishes the context through which the project addresses the requirements and investigates the practicality of a proposed solution. The feasibility study is used to determine if the project should get the go-ahead. If the project is to proceed, the feasibility study will produce a project plan and budget estimates for the future stages of development.

Requirements Analysis Phase

This phase formally defines the detailed functional user requirements, using high-level requirements identified in the Initiation and Feasibility Phases. In this phase, the requirements are defined to a sufficient level of detail for systems design to proceed. Requirements need to be measurable, testable, and relate to the business need or opportunity identified in the Initiation Phase.

Design and Development Phase

During this phase, the system is designed to satisfy the functional requirements identified in the previous phase. Since problems in the design phase can be very expensive to solve in later stages of the software development, a variety of elements are considered in the design to mitigate risk. These include:

Identifying potential risks and defining mitigating design features

Performing a security risk assessment
Developing a conversion plan to migrate current data to the new system
Determining the operating environment

Implementation, Documentation and Testing Phase

For Bureau of Customs Information Systems, as part of the implementation phase, updated detailed documentation will be developed and will include all operations information needed by MISTG, including detailed instructions for when systems fail. Bureau of Customs Information Systems may not be moved into the production environment without this documented information.

Testing includes unit, integration, and system testing to ensure the proper implementation of the requirements.

The requirements will be documented and will then be tested. All components deployed for cloud architecture are based on a defined secure standard from the vendor and security best practices and goes through a change control process that includes configuration, testing, and QA, before it is deployed in Production.

Operations and Maintenance Phase

System operations and maintenance is ongoing. Bureau of Customs conducts an annual review with Stakeholders. The system is monitored for continued performance in accordance with user requirements and needed system modifications are incorporated when identified, approved, and tested. When modifications are identified, the system may reenter the planning phase.

Policy Review

This policy will be reviewed at least annually by Management for effectiveness and to ensure its continued use and relevance as part of the Bureau of Customs information security management system (ISMS).

COMPLIANCE AND REPORTING

All applications are reviewed at predetermined checkpoints of the SDLC by the Information Systems Analyst or their designate. Any deviations are identified, and corrective action is determined prior to the application being released to production. Electronic authorization indicating standards have been met is required before a new or modified application can be released to production.
MISTG always enforces this Policy and the related Standards. Anyone who has reason to suspect a deliberate and / or significant violation of this Policy is encouraged to promptly report it to the MISTG Help Desk. Policy violations that come to the attention of the MISTG Help Desk will be escalated to the Chief, System Development Division. Policy violations will be assessed, and action taken to remediate the violation subject to collective agreements and / or other contractual conditions.

Where Policy violations are considered severe and / or cannot be easily remediated, the incident will be escalated to the Director, MISTG-PSDS for further action. Periodically, the Deputy Commissioner, MISTG will provide to Executive Committee a summary of all policy violations.

Policy owner:	Liberty Plana, Chief, MISTG-SDD
Authorized by:	Atty. Kriden Balgomera, Deputy Commissioner, MISTG
Created by:	Francis Aquino, Information Systems Analyst
Approved by:	BOC Executive Committee
Effective date:	August 2020
Next review:	July 2021
Revision history:	V1.3
Related documents:	CMO No. 04-2019 Bureau of Customs Citizen's Charter 2019

MISTG Memo No. 08 - 2020 p. 9

MASTER COPY

BUREAU OF CUSTOMS

CITIZEN'S CHARTER

2019 (1st Edition)

23. Request for Simple System Development (Stand-Alone System)

The SDD will design, develop, test and deploy a simple software application system customized for the use of a group within the Bureau and/or the public.

Office or Division:	**SYSTEMS DEVELOPMENT DIVISION (SDD)**
Classification:	Highly Technical
Type of Transaction:	G2G - Government to Government
Who may avail:	BOC Concerned Office

CHECKLIST OF REQUIREMENTS	**WHERE TO SECURE**
Letter Request (1 original)	Applicant
Memorandum Order (1 original)	Applicant
Customs Memorandum Circular (1 original)	Applicant
Update Notice Form (1 original)	Applicant

CLIENT STEPS	**AGENCY ACTIONS**	**FEES TO BE PAID**	**PROCESSING TIME**	**PERSON RESPONSIBLE**
1. Make request for system development	1.1 Receive the letter request 1.2 Log the transaction to the DTS 1.3 Review/check the completeness of the request	None	15 minutes	*Staff/Receiving Clerk* MISTG
	1.4 Issue directive for the development plan	None	20 minutes	*Deputy Commissioner* MISTG

	1.5 Check the complexity of the project; define the scope of the concept	None	1 day	*Staff* Systems Development Division
	1.6 Develop a project management plan	None	2 days	*Staff* Systems Development Division
	1.7 Analyse user's need and develop user's requirement. Create a detailed functional requirement	None	3 days	*Staff* Systems Development Division
	1.8 Transform detailed requirement into complete detailed System Design	None	3 days	*Staff* Systems Development Division
	1.9 Convert design into complete information system - Installing system environment - Creating and testing database 1.10 Coding, compiling, refining	None	7 days	*Staff* Systems Development Division

	program			
TOTAL		**None**	**16 days, 35 minutes**	

24. Request for Software Quality Testing

The Software Quality Assurance (SQA) Team under the SDD will conduct tests to ensures that developed software meets and complies with defined technical specifications.

Office or Division:	**SYSTEMS DEVELOPMENT DIVISION (SDD)**
Classification:	Highly Technical
Type of Transaction:	G2G - Government to Government
Who may avail:	Management Information System and Technology Group (MISTG)

CHECKLIST OF REQUIREMENTS	**WHERE TO SECURE**
Update Notice Form (UNF) (1 original)	Applicant
Business Rules (1 original)	Applicant
Systems Design/Flowchart (1 original)	Applicant
Systems Specification (1 original)	Applicant
System Walkthrough	

CLIENT STEPS	**AGENCY ACTIONS**	**FEES TO BE PAID**	**PROCESSING TIME**	**PERSON RESPONSIBLE**
1. SDD submits the documentary requirements to the SQA team.	1.1 Receives and assigns the documentary requirements to software testers for evaluation	None	10 minutes	*Information Technology Officer (ITO) III* Systems Development Division (SDD)

	1.2 Verifies all the documentary requirements	None	5 minutes	*SQA Team* SDD
2. SDD conducts system's walkthrough	2.1 Attends the system's walkthrough	None	1 hour	*SQA Team* SDD
	2.2 Tests the quality of the system	None	10 days	*SQA Team* SDD
	2.3 Prepares Test Incident Report (TIR) for every bug that will be encountered	None	10 minutes	*SQA Team* SDD
3. SDD fixes the reported bug(s) and notifies the SQA Team if it's already resolved	3.1 Tests each resolved TIR	None	20 minutes	*SQA Team* SDD
	3.2 Conducts regression testing if all of the TIRs were already resolved	None	2 days	*SQA Team* SDD
	3.3 Concludes completion of testing if there's no error encountered after the regression testing	None	1 hour	*SQA Team* SDD
	3.4 Signs and compiles the Update Notice Form (UNF)	None	10 minutes	*Chief* SDD *Director* PSDS
	3.5 Notifies SDD Chief via email that the system is ready for implementation	None	10 minutes	*ITO II* SDD

	3.6 Provides UNF copy to SDD and TSD			
TOTAL		**None**	**12 days, 3 hours, 5 minutes**	

25. Request for Statistical Data

The SDD extracts, compiles and furnishes the requested import data upon written request of the proper party.

Office or Division:	**SYSTEMS DEVELOPMENT DIVISION (SDD)**
Classification:	SIMPLE
Type of Transaction:	G2C - Government to Citizen G2B - Government to Business
Who may avail:	Stakeholders with BOC transactions, Other Government Agencies

CHECKLIST OF REQUIREMENTS	**WHERE TO SECURE**
Letter Request (1 original) indicating the following:	Applicant
a. Details of requested data (i.e., period, commodity code)	
b. Reason why the data is being requested	
Data Privacy Officer approval, whenever applicable (1 original)	Data Protection Officer

CLIENT STEPS	**AGENCY ACTIONS**	**FEES TO BE PAID**	**PROCESSING TIME**	**PERSON RESPONSIBLE**