U.S. Department of Housing and Urban Development (HUD)

Handbook 3253.1

Change Management Policy

August 2022

Policy Revision History

Issue	Date	Pages Affected	Description
Initial Draft	July 6, 2021	All	Initial Version
Final Draft	November 3, 2021	All; Incorporated feedback from IOO and OITS	Final Draft Version 1.0
Finalized Policy	August 2, 2022	All; Incorporated feedback from Departmental Review	Final Version 1.0

Table of Contents

HUD Change Management Policy

1.0 Background

The HUD Office of the Chief Information Officer (OCIO) supports a large and complex IT environment consisting of networks, servers, applications, software, databases, and services. A change to the configuration of any of these items may introduce risk to HUD's availability, capacity, reliability, and performance. To mitigate these risks and also improve operational efficiencies, HUD must manage all system configuration changes throughout the product or system lifecycle.

The primary Change Management principles include:

- Changes to an approved configuration are accomplished using a systematic, measurable change process
- Justifying the need for a change provides the rational to commit resources required to document, process, and if approved, implement the change
- A unique change identifier enables verification and tracking of the request for change and the status of implementation
- Classification of a requested change determines the appropriate level of review and the applicable change disposition authority
- The request for change document must be clear and comprehensive from the technical, cost, and scheduling perspectives.

This document formalizes the IT Change Management policy that is designed to ensure that changes are managed and tracked from start to finish and in a manner that addresses these principles.

1.1 Program Scope and Objectives

This document describes the formal Information Technology (IT) policy for Change Management (ChM) that complies with federal guidance and aligns with industry standards and ensures that all changes to HUD's IT environment is recorded and managed in a controlled way. It provides the purpose, scope, authority, and mandates for implementing change management requirements.

The objective of Change Management is to ensure that:

- Standardized methods and procedures are used for efficient and prompt handling of all changes to control the HUD IT infrastructure and business applications to minimize the impact of any related incidents upon the service.
- Configuration baselines are maintained and controlled
- Change requests are reviewed and approved prior to implementation
- Traceability is maintained for the life of a product
- Interfaces are identified and controlled
- Products and all product configuration information and document are kept consistent

The scope of Change Management covers changes to all IT products and associated configuration items (CIs) across the whole service lifecycle.

2.0 Purpose

The purpose of this Policy is to establish formal requirements to manage changes to IT systems and applications to ensure that a consistent and systematic approach is used for implementing changes, control the lifecycle of all changes, and enabling beneficial changes with minimum disruption to IT services. This includes establishing a Departmentwide Change Management process that identifies responsibilities, compliance requirements, and overall principles of Change Management to support information technology management across the IT organization.

Change Management aims to manage the process of change and limit the introduction of errors into HUD's IT systems and applications. The OCIO Configuration Change Management Board (CCMB)[1] conducts and implements Change Management policies, practices, and procedures to:

- Establish a common understanding for HUD as an agency and for HUD's customers and vendors regarding HUD's approach to the assessment of risk, change impact, resource requirements, and change approval. This approach is required to balance the need for change against the impact of the change.
- Ensure a standard, formal process is used for implementing all changes to HUD's IT environment, systems, and applications.
- Ensure that Change Management processes receive high visibility and open channels of communication to promote smooth transitions that support successful changes and offer options when a change is not successful.
- Provide a comprehensive picture of the organization-wide impact of change and enable appropriate planning activities that should include contingency plans and communications.

3.0 Applicability

The Change Management Policy is applicable to all HUD organizations, HUD employees, IT contractors, and other stakeholders using IT assets or having roles and responsibility for change management, oversight, and successful day-to-day operations of HUD's IT applications and systems.

This Policy is applicable to any change that might affect Departmental products, systems, applications, and services in the IT environment. This includes changes to all architectures, applications, software, tools, and documentation, as well as changes to all configuration items across the whole service lifecycle. Reviewing requests for changes to a product allows HUD to determine:

- Any impacts to security
- If the design, development or test efforts will be impacted
- If databases or architecture is impacted
- If product support requirements are impacted
- If performance and reliability are impacted
- If internal or external interfaces are affected
- If current work schedule, scope, delivery or schedule are affected
- If the change offers sufficient value to HUD or does it impact total project or product costs
- If and what product documents are affected
- If HUD asset standards and compatibility requirements are impacted.

[1] CCMB website (available at http://hudatwork.hud.gov/HUD/cio/po/i/it/sd/devlife/def/CCMB/ccmb)

4.0 Rescission

This policy does not rescind any other policy or document. This is HUD's Change Management Directive, version 1.0. This document will be reviewed annually, and rescission information will be updated as necessary.

5.0 Effective Implementation Date

This policy is effective immediately upon the date of approval.

6.0 Authority

The Chief Technology Officer is responsible for managing and overseeing HUD's configuration management (CM) program, which includes managing configurations throughout a product or system life cycle. The CCMB and associated governance is responsible for the development, implementation, and maintenance of this policy. Ensuring compliance with this policy, including updates, rests with the CCMB Chair under the OCIO Chief Technology Officer. All proposed changes to this policy must be submitted to the CCMB for approval.

7.0 Policy

The Change Management policy complies with the following guidance and policies:

- NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
- HUD Handbook 2400.25, IT Security Policy
- HUD Handbook 3252.1, Software Configuration Management Policy
- HUD Secure Configuration Management Directive[2]

All changes to a documented, approved configuration must be accomplished using a systematic, measurable change process. To maintain accurate information and status of system configurations, any proposed change to a HUD system, application or service (e.g., Production, Development, Test, Disaster Recovery, etc.), must be recorded as a Request for Change (RFC). The RFC is used to manage changes and must contain clear and comprehensive information from technical, cost and scheduling perspectives. All changes must undergo a solution validation and impact analysis, and verification that the information is accurate and complete prior to submission for disposition determination. All changes must be authorized by the CCMB or CCMB-authorized disposition official prior to implementation.

Once an RFC is approved, changes are deployed in the approved schedule and timeframe identified within the RFC. Any modifications to an RFC must be submitted as an RFC revision and submitted for disposition.

7.1 Request for Change Assessments

All RFCs must be submitted to the CCMB mailbox (CCMBRequests@hud.gov) using the Request for Change (RFC) template[3]. To be considered a valid request, the template must be completed in

[2] The HUD Secure Configuration Management Directive outlines the identification of secure baselines for HUD IT systems, handling of configuration deviations, configuration monitoring, and changes to configurations (available at http://hudatwork.hud.gov/HUD/cio/doc/SecureConfigMgt).

[3] RFC template and instructions are available on the CCMB website (available at http://hudatwork.hud.gov/HUD/cio/po/i/it/sd/devlife/def/CCMB/ccmb)

entirety and must include an assessment of the following:

- Solution alternatives, if applicable, and validation of technical proposal;
- Impact Analysis on identified costs, schedule, training, business, and draft implementation plan;
- Risk considerations related to technical, operational, support, schedule, and costs; and
- Impact of not approving the RFC.

All RFCs received by the CCMB that are determined to be incomplete or lack sufficient information will be returned to the RFC originator without consideration.

7.2 Change Request Disposition

An effective, well-defined configuration change control process assures that all changes to controlled baselines, no matter how small or seemingly insignificant, are reviewed by the applicable configuration change control authority. Without an effective configuration change control process, the Department runs the risk of delivering products, systems or services with configurations that:

- Are technically inadequate and fail to meet specified performance requirements
- Are not logistically or operationally supportable
- Result in wasted resources
- Fail to provide an accurate historical record as a basis for future change
- Fail to utilize contracted funds properly to address lifecycle costs
- Result in inconsistencies across configuration items

Therefore, the RFC must be completed for each change to a HUD product, system or service and is the basis for an approval or disapproval decision by a disposition authority. The RFC, including all technical, schedule, and cost impacts, is presented to the disposition authority for evaluation and the requested change as either approved, deferred for more research, or disapproved. When the decision is disapproval, the RFC is archived without further action. When the decision is approval, the change proceeds to change implementation and the approval is documented into the RFC template. The disposition results are then disseminated to the affected group and action items are tracked.

7.3 Request for Change Status Accounting

The purpose for all configuration management activities is to make sure that product or system definition information is sufficiently documented to produce, replicate, and support a product or system throughout its life cycle. Change status accounting confirms the state of each change, which enables information about product readiness for delivery and use and servicing and also allows correct scheduling of service-related changes and timely availability of replacement parts and materials needed for servicing.

Therefore, the RFC originator is responsible for providing current implementation information to the CCMB for all approved changes and for capturing the product configuration information as tasks are performed. When changes are implemented, the success or failure of the implementation must be recorded on the RFC. Changes considered unsuccessful include changes not implemented as planned; changes backed out (partial or in entirety), changes not implemented per schedule; and changes causing incidents. All unsuccessful changes must be reviewed by CCMB to determine the cause of the failure and plan remediation actions for the future. All change status information will be retained and available to the business and customers throughout the product life cycle.

7.4 Managing Change Variance

A request for variance (RFV) is identified, classified, documented, coordinated, evaluated and dispositioned when a temporary departure from a specified baseline requirement is necessary. A request for variance must describe the non-conforming product, or material, that departs from approved product definition information or does not meet baseline requirements. Variances may affect one or more units or may be implemented for a specific period of time without changing the approved baseline. A variance can be requested before production resulting in the creation of a non-conforming product for a specific period of time, or the more common after production when one or more products is found to be non-conforming. When a variance exists, it must be documented, and limited to as few production units as possible.

RFVs must be submitted to the to the CCMB mailbox (CCMBRequests@hud.gov) for consideration by the appropriate disposition authority. The RFV must identify pertinent impact information, such as test information, analyses and other technical documentation that provides supporting rationale for assertions made in the request for variance. An integral part of the processing of any variance is the follow-on investigation of the cause(s) of the variance to eliminate the cause(s) and prevent a recurrence. In describing the need for the variance, an explanation of why it is not possible to comply with the configuration documentation within the specified delivery schedule and why a variance is proposed in lieu of a permanent design change.

An approved request for variance gives specific written authorization to allow a variance from a particular technical requirement(s) documented in the current baseline product definition information for a specific unit, a specific number of units, or a specified period of time. A variance differs from a change in that the variance does not implement a revision to baseline product definition information. The variance evaluation must address the technical impacts of the variance and evaluate the effectivity, cost, schedule, and product support.

If the decision is disapproval of the variance, it may be archived without further action, the variance is returned to the initiator for further clarification (change repair procedures, quantity, etc.), or modify the purpose (need) of the variance and the non-conforming product (i.e. change to repair vice use-as-is). If the decision is approval, the variance proceeds to the implementation and verification stage of this process.

8.0 Roles and Responsibilities

8.1 Configuration Change Management Board (CCMB)

- The CCMB is responsible for the development, implementation, and maintenance of the Change Management Policy, including all future policy updates.
- The CCMB must provide a repository for all change and variance requests and will monitor as identified.
- The CCMB is the RFC disposition authority for all applications, as well as any product, platform, or service that resides outside of HUD’s IT Infrastructure.
- The CCMB is composed of OCIO representatives from all areas of IT that advise on the RFC assessment, prioritization, and scheduling of changes. Based on the RFC review, the CCMB must either:
    - Approve the RFC and allow the change to be submitted into HUD’s Release Management process
    - Disapprove the RFC and disallow the change to progress onto Release Management
    - Deferred the RFC to request additional information before making final determination or to allow a related activity to be completed

8.2 Office of IT Security (OITS)

- OITS is responsible for establishing and providing guidance on cybersecurity policies and regulations
- OITS will review RFCs and RFVs summitted to the disposition authorities to confirm compliance with cybersecurity policies and requirements and to ensure that any security risks are adequately addressed in submitted information.
- OITS can reject an RFC or RFV based on the negative impact to the confidentiality, integrity, and availability of any HUD system, product, service, or interface.

8.3 Office of Infrastructure and Operations (IOO)

- IOO is responsible for the operation and management within HUD's infrastructure and is the disposition authority for HUD Infrastructure change and variance requests.
- IOO is required to implement a change and variance management process for infrastructure that complies with this policy.
- IOO must provide copies of all RFCs and RFVs to the CCMB.
- IOO must determine if the RFC or RFV is accurate and complete and any submission that does not meet the quality review will be returned to the RFC originator for action.
- IOO must conduct an initial review of the risk, technical, security, and business impact assessment information for the infrastructure RFCs and RFVs.
- IOO must submit copies of all RFCs and RFVs to the CCMB for document retention
- IOO must confirm status information for all infrastructure RFCs and RFVs to the CCMB.
- IOO must update configuration documentation as necessary to reflect changes to the infrastructure products and services.

8.4 RFC and RFV Originator

The RFC or RFV originator is typically the designated HUD System Owner[4], IT Project Manager, IT Program Manager, or Technical Point of Contact (TPOC) responsible for the system, application, or service. The RFC and RFV originator is responsible for supporting the planning, designing, and testing required for an RFC or RFV. Upon approval from the disposition authority, the RFC originator is responsible for implementing the change or variance within HUD's standardized Testing, Release Management and life cycle of the system, application, or service.

The role of the RFC Originator includes the following responsibilities:

- Submitting a complete and accurate RFC or RFV to the CCMB.
- Advancing and executing the RFC or RFV through the Change Management process. This includes responsibility for coordinating the assessment of the RFC/RFV and ensuring that the tasks necessary to complete the RFC are planned, scheduled, resourced, and executed as approved by the CCMB.
- Acting as or coordinating with the Subject Matter Experts (SMEs) supporting RFC or RFV and providing specific expertise to the various technical and business aspects of the proposed change.
- Providing RFC and RFV status information to the CCMB.
- Update configuration documentation as necessary to reflect changes to the application.

[4] HUD Handbook 2400.25, HUD IT Security Policy; Section 7.0 Roles and Responsibilities (https://www.hud.gov/sites/dfiles/OCHCO/documents/240025CIOH.pdf)

9.0 Authorities and References

- NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
- HUD Handbook 2400.25, IT Security Policies
- HUD Handbook 3252.1, Software Configuration Management Policy
- Software Configuration Management Procedures http://hudatwork.hud.gov/HUD/cio/po/i/it/security/cmb/cmbprocedures
- HUD Secure Configuration Management Directive http://hudatwork.hud.gov/HUD/cio/po/i/ociopolicies
- HUD Configuration Change Management Board http://hudatwork.hud.gov/HUD/cio/po/i/it/sd/devlife/def/CCMB/ccmb
- SAE-EIA-649C, Configuration Management Standard (https://www.sae.org/standards/content/eia649c/)

10.0 Definitions

Term	Definition
Approved document	A change or variance request that has been approved by the appropriate disposition authority and is the official version of the document until replaced by another approved version.
Change	A proposed change to an approved configuration for which HUD is the current change authority and affects any physical or functional baseline and associated configuration documentation.
Change Request	Information describing the justification to request a change submitted to the CCMB for disposition.
Configuration	A collection of an item's descriptive and governing characteristics that can be expressed in functional terms (i.e. what performance the item is expected to achieve) and in physical terms (i.e. what the items should look like and consist of when built). Configuration represents the requirements, architecture, design and implementation that define a particular version of a system or system component.
Configuration Baseline	An agree-to description of the attributes of a product, at a point in time, which services as a basis for defining change and includes the currently approved and released configuration documentation.
Configuration Change Management Board (CCMB)	HUD's official forum composed of technical, logistics, acquisition, management, and administrative personnel who recommend approval or disapproval of a proposed change to, and variance from, an item's approved configuration.
Configuration Control	The configuration management activity concerning the systematic proposal, justification, evaluation, coordination, and disposition of proposed changes; and the implementation of all approved and released changed into (a) the applicable configurations of a product, (b) associated product information, and (c) supporting and interfacing products and their associated product information.
Configuration Documentation	Technical documentation that identified and defines a product's performance, functional and physical attributes.
Configuration Item	A product, or major component in the product structure of a complex product, that provides functions of importance to the end product. The CI designation is a convenient way to refer to items that have separate requirements specifications, may be separately developed, and are an item to which the effectivity of changes to its components is addressed.
Configuration Management	The function that ensures changes to a configuration baseline are properly identified, recorded, evaluated, approved or disapproved, and incorporated and verified as appropriate.
Configuration Status Accounting	The recording and reporting of the established product configuration information, the status of proposed changes, and the implementation of approved changes and changes occurring to the product due to operation and maintenance. Configuration status accounting also includes assurances that the information is current, accurate and retrievable.
Defect	Any nonconformance of a characteristic to specific requirements

Term	Definition
Deficiency	Condition or characteristic in any product or the documentation of any product which is not in accordance or does not reflect accurate information with the product’s current approved configuration.
Disposition Authority	The organization or person authorized to approve: 1) A configuration change to a product and 2) Changes to product definition information and other related documents
Effectivity	A designation, defining the product range (e.g., serial numbers, IP addresses, batch numbers, model, date or event) at which a specific production configuration applies, a change is to be or has been affected, or to which a variance applies.
Interface	The place, situation, or way in which two things act together or affect each other or the common boundary of two or more products. Also, the performance, functional, and physical characteristics required to exist at a common boundary.
Life Cycle Management	A basic principle of management of the sequence of stages that an information technology product goes through during the time span of its ownership. The main stages of an IT asset's life-cycle are planning, procurement, deployment, usage, upgrade, decommission, and disposition
Life Cycle Cost	The total cost to the tasking activity of acquisition and ownership of a product over its life cycle. As applicable, it includes the cost of development, acquisition, support, maintenance, and decommissioning
Major Change	A change with significant impacts to the functional and physical interchangeability and supportability of the product
Minor Change	A change that has little or no significant impact
Non-Recurring Costs	A one-time cost that will be incurred if the change is approved and is independent of the quantity of items changed (such as cost of redesign or development testing)
Process	A set of interrelated tasks that together, transform inputs into outp
Product	The result of a process. There are five generic product categories: • Hardware; • Software; • Processed materials; • Documentation (e.g., specifications, drawings, test procedures, publications, version description documents) and • Services
Product Attributes	Functional and physical characteristics, including performance and interface features, of a product. For a software product, the “product attributes” can be a list of files and file revisions.

Term	Definition
Product Baseline	The approved technical documentation and work product (i.e., "build-to" and "code-to" items such as specifications, drawings, software code, Interface Control Documents, and related materials) which describes a CI during the production, fielding/deployment and operational support phases of its life cycle.
Recurring Costs	Costs that are incurred on a per-unit basis for each item changed or for each service or document required.
Release	The designation by the originating activity that a document representation or software version is approved by the appropriate authority and is subject to configuration change management.
Request for Change	Information by which a change is proposed, described, justified, and submitted to the disposition authority.
Request for Variance	Information by which a request is proposed to request permission to temporarily depart from the product requirements.
Revision	The result of updating a product or production configuration information (see Version)
Variance	Temporary departure from the production definition information for a product.
Verification	All examinations, tests, and inspections necessary to verify that a product performs satisfactorily as intended and confirms that it meets specified requirements.
Version	A supplementary identifier used to distinguish a changed body or set of data from the previous configuration with the same identifier.

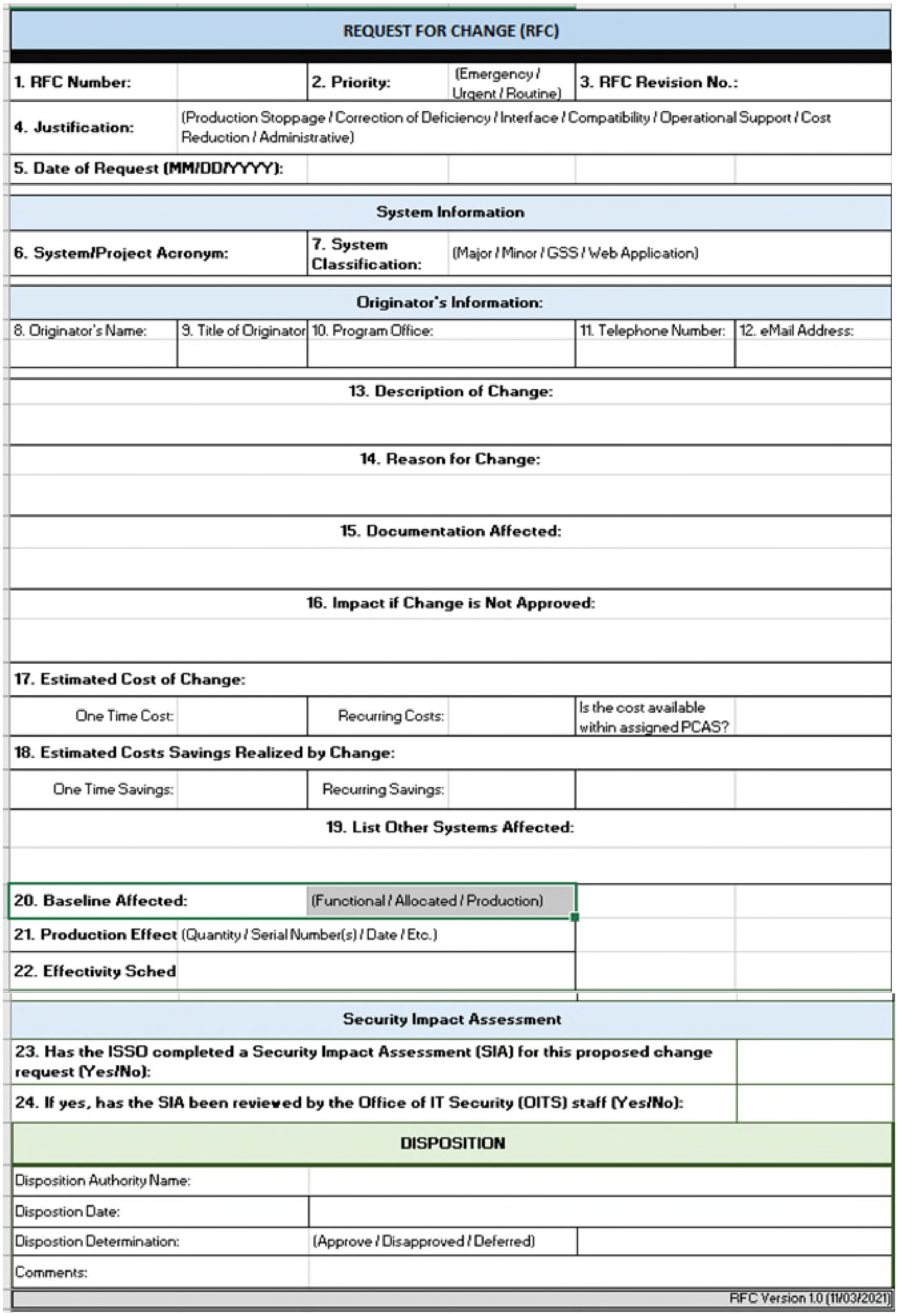
11.0 Acronyms

Acronym	Definition
CCMB	Configuration Change Management Board
ChM	Change Management
CI	Configuration Item
CM	Configuration Management
IT	Information Technology
IOO	Office of Infrastructure and Operations
OCIO	Office of the Chief Information Officer
OITS	Office of IT Security
RFC	Request for Change
RFV	Request for Variance
TPOC	Technical Point of Contact
SME	Subject Matter Expert

Appendix A Request for Change (RFC) Template

The RFC Template (provided as a picture below) and RFC Template Instructions are available on the Office of the Chief Information Officer (OCIO) Configuration Change Management Board (CCMB) website:

http://hudatwork.hud.gov/HUD/cio/po/i/it/sd/devlife/def/CCMB/ccmb

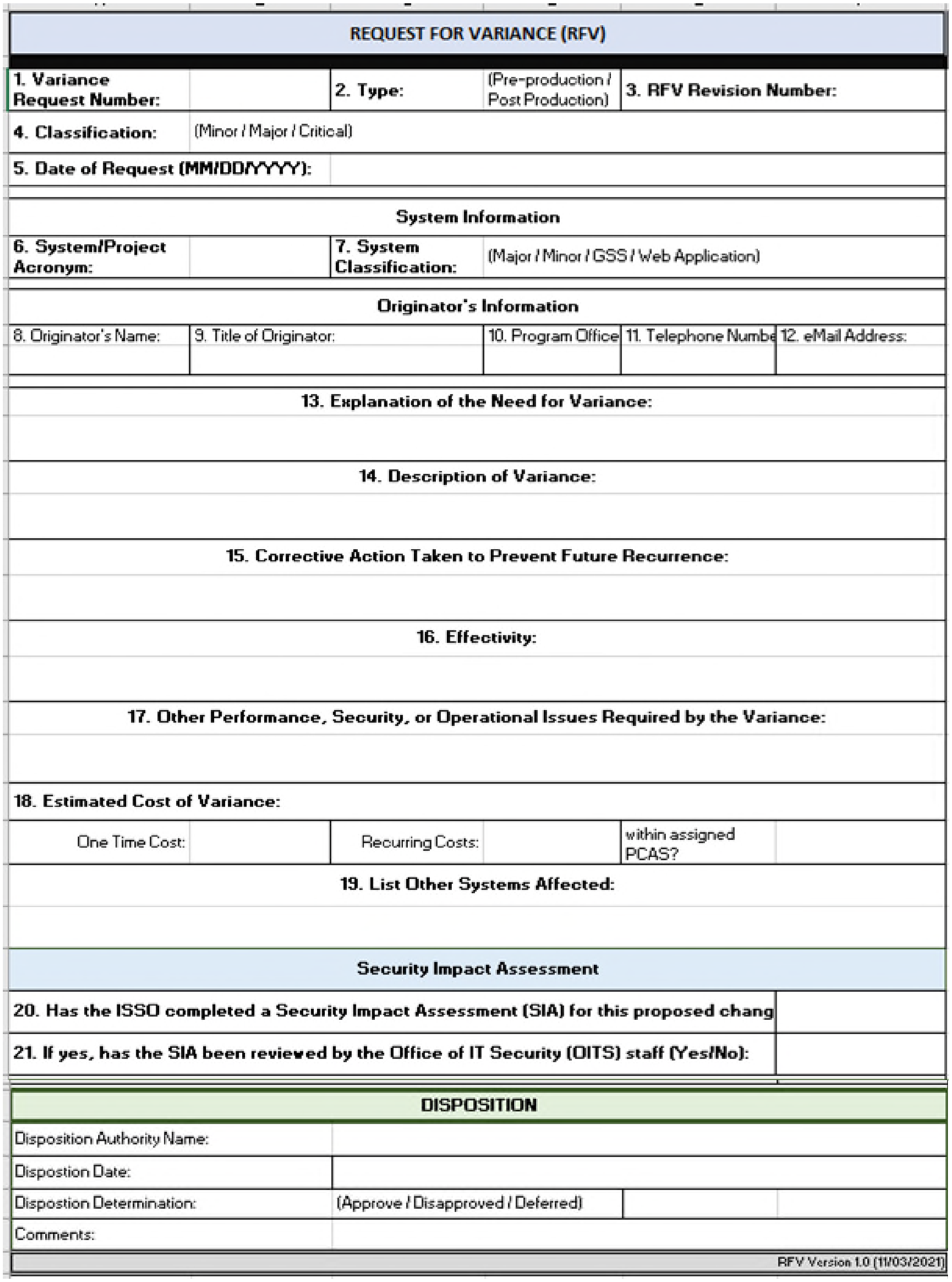


REQUEST FOR CHANGE (RFC)					
1. RFC Number:		**2. Priority:**	(Emergency / Urgent / Routine)	**3. RFC Revision No.:**	
4. Justification:	(Production Stoppage / Correction of Deficiency / Interface / Compatibility / Operational Support / Cost Reduction / Administrative)				
5. Date of Request (MM/DD/YYYY):					
System Information					
6. System/Project Acronym:		**7. System Classification:**	(Major / Minor / GSS / Web Application)		
Originator's Information:					
8. Originator's Name:	9. Title of Originator	10. Program Office:		11. Telephone Number:	12. eMail Address:
13. Description of Change:					
14. Reason for Change:					
15. Documentation Affected:					
16. Impact if Change is Not Approved:					
17. Estimated Cost of Change:					
One Time Cost:		Recurring Costs:		Is the cost available within assigned PCAS?	
18. Estimated Costs Savings Realized by Change:					
One Time Savings:		Recurring Savings:			
19. List Other Systems Affected:					
20. Baseline Affected:		(Functional / Allocated / Production)			
21. Production Effect	(Quantity / Serial Number(s) / Date / Etc.)				
22. Effectivity Sched					
Security Impact Assessment					
23. Has the ISSO completed a Security Impact Assessment (SIA) for this proposed change request (Yes/No):					
24. If yes, has the SIA been reviewed by the Office of IT Security (OITS) staff (Yes/No):					
DISPOSITION					
Disposition Authority Name:					
Dispostion Date:					
Dispostion Determination:		(Approve / Disapproved / Deferred)			
Comments:					
					RFC Version 1.0 (11/03/2021)

Appendix B Request for Variance (RFV) Template

The RFV Template (provided as a picture below) and RFV Template Instructions are available on the Office of the Chief Information Officer (OCIO) Configuration Change Management Board (CCMB) website:

http://hudatwork.hud.gov/HUD/cio/po/i/it/sd/devlife/def/CCMB/ccmb



REQUEST FOR VARIANCE (RFV)					
1. Variance Request Number:		**2. Type:**	(Pre-production / Post Production)	**3. RFV Revision Number:**	
4. Classification:	(Minor / Major / Critical)				
5. Date of Request (MM/DD/YYYY):					
System Information					
6. System/Project Acronym:		**7. System Classification:**	(Major / Minor / GSS / Web Application)		
Originator's Information					
8. Originator's Name:	9. Title of Originator:		10. Program Office	11. Telephone Numbe	12. eMail Address:
13. Explanation of the Need for Variance:					
14. Description of Variance:					
15. Corrective Action Taken to Prevent Future Recurrence:					
16. Effectivity:					
17. Other Performance, Security, or Operational Issues Required by the Variance:					
18. Estimated Cost of Variance:					
One Time Cost:		Recurring Costs:		within assigned PCAS?	
19. List Other Systems Affected:					
Security Impact Assessment					
20. Has the ISSO completed a Security Impact Assessment (SIA) for this proposed chang					
21. If yes, has the SIA been reviewed by the Office of IT Security (OITS) staff (Yes/No):					
DISPOSITION					
Disposition Authority Name:					
Dispostion Date:					
Dispostion Determination:	(Approve / Disapproved / Deferred)				
Comments:					
				RFV Version 1.0 (11/03/2021)	

Appendix C Change Request Impact Analysis

NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf) provides a sample template for a Security Impact Analysis that can be considered when conducting an analysis or impact related to a configuration change request.

Other impact considerations to consider include:

- Are customers affected?
- Does this affect regulatory requirements?
- Is the system performance, reliability, or security affected?
- Will any system interfaces be affected?
- Does this affect current work, budget, scope, deliverables, and/or schedule?
- Are resources available to implement patch?
- What system documents are affected?
- Will the system design, development, test, or O&M efforts be affected?
- Will tools and/or standard processes be impacted?
- Is sufficient value added?