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

Handbook 3254.1

Enterprise Patch Management Policy

August 2022

Policy Revision History

Issue	Date	Pages Affected	Description
Initial Draft	March 25, 2021	All	Initial Version
Revised Draft	July 1, 2021	All	Update of the policy and its components to reflect changes and enhancements in IT management disciplines and lessons learned from their use by OCIO. Incorporated OITS and IOO comments.
Revised Draft	August 12, 2021	Various	Addresses additional comments from OITS related to patch testing, impact analysis and roles and responsibilities. Added Appendix C Change Impact Analysis
Final Draft	November 3,2021	Various	Final Draft Version 1.0 for Departmental Clearance
Final Policy	August 2, 2022	Various	Incorporated feedback from Departmental Review. Final Version 1.0

Table of Contents

HUD Enterprise Patch Management Policy

1 Introduction

The U.S. Department of Housing and Urban Development (HUD) is responsible for ensuring the confidentiality, integrity, and availability of its systems, data and the sensitive customer data stored on its systems. HUD must provide appropriate protection against cybersecurity threats that could adversely affect the security of the system or its data entrusted on its systems. Effective implementation of this policy supports HUD's configuration management program and limits the exposure and effect of common cybersecurity threats to the systems within this scope.

Patch management is the process of identifying, acquiring, installing, and verifying patches for products and systems. Patches[1] correct security and functionality problems in software and firmware. From a security perspective, patches are significant because they mitigate software flaw vulnerabilities, thereby reducing the opportunities for exploitation. However, patches serve other purposes that include adding new features to software and firmware, including enhanced security capabilities.

Regular application of vendor-issued critical security updates and patches are necessary to protect HUD's data and systems from malicious attacks and erroneous functions. All electronic devices connected to the network including servers, workstations, firewalls, network switches, and routers, tablets, mobile devices, and cellular devices routinely require patching for functional and secure operations.

2 Purpose

This policy establishes and emphasizes a "*risk-based*" approach for ongoing, and consistent system and application of regular security updates and patches to operating systems, firmware, productivity applications, and utilities software[2]. Regular updates are critical to maintaining a secure operational environment.

This policy establishes HUD's policy for the management and application of vendor-issued critical security updates and patches that are necessary to protect HUD's data and systems from malicious attacks and erroneous functions. The Enterprise Patch Management Policy integrates a variety of related IT methods, mandates, and practices into a common life cycle framework. The essential components of the Enterprise Patch Management Framework are defined through a suite of supporting processes, guidelines, and roles and responsibilities. The framework and its components will be continuously updated to reflect changes in the disciplines and lessons learned from their use by HUD organizations.

[1] Patches are additional pieces of code developed to address problems (commonly called "bugs") in software.
[2] OMB M-16-12, for the purposes of the memorandum, defines IT software to includes the commercial and commercial-off-the-shelf (COTS) software licenses (perpetual and term licenses) and maintenance (maintenance contracts, software assurance, upgrades, patches, and limited helpdesk support).

3 Applicability

This policy applies to all commercially available hardware and software owned or managed by HUD or by contractors on behalf of HUD . This includes all systems that fulfill HUD's mission or business requirements regardless of operational location.

This policy also applies to custom software patches development required to address vulnerabilities in HUD's legacy application custom code. HUD staff are encouraged to ensure that system support resources are available to comply with all configuration management lifecycle support requirements, including patch management.

4 Rescission

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

5 Effective Implementation Date

This policy is effective immediately upon the date of approval.

6 Policy

HUD accepts patch alerts and patches from appropriate vendors, the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) and other federally authorized sources. Once received, the patches shall be prioritized based on the risk associated with the affected system(s) and the nature of the vulnerability being patched. The table below identifies the standard timeframes for installing patches:

Patch Priority	System Patch Distribution	Patch Installation/Application Completion Timeframe:
DHS Emergency Directive[3]	Distribution shall begin as directed	100% of systems – Date defined in Directive
Critical	Distribution shall begin within 72 hours of patch availability.	100% of systems - 15 days
High	Distribution shall begin within 5 business days of patch availability.	100% of systems - 30 days
Medium	Distribution shall begin within 30 calendar days of patch availability.	100% of systems - 90 days
Low	Distribution shall begin within 90 calendar days of patch availability.	100% of systems - 150 days

[3] The Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS) develops and oversees the implementation of "binding operational directives" and "emergency directives," which require action on the part of certain federal agencies in the civilian Executive Branch; https://cyber.dhs.gov/directives/; Please note that patch management may not address all required actions identified in a DHS Emergency Directive to address a vulnerability.

Application of security patches is a required activity for all HUD systems and therefore, all system components and software shall be protected from known vulnerabilities by installing applicable vendor-supplied security patches.

All patches identified for an approved configuration will be accomplished using a systematic, measurable change process. To maintain accurate information and status of system configurations, patches must be recorded as a Request for Change (RFC)[4]. The RFC template details are provided in Appendix A. The RFC is used to manage changes and the information identified must be clear, accurate and comprehensive from the technical, cost and scheduling perspectives. All RFCs must also include an impact analysis[5], and submitted for review and disposition determination.

System components and devices attached to the production environment shall be regularly maintained by applying critical security patches as prescribed by the vendor and federal guidance. If a critical patch requires more than 72 hours for distribution, a Plan of Action and Milestones (POA&M)[6] must be created for the system and stored and monitored in Computer Security Assessment and Management (CSAM). For HUD infrastructure systems and products, the Office of the Chief Informatio Officer (OCIO) Information Systems Security Office (ISSO) is responsible for creating, submitting and monitoring the POA&M. For HUD applications, HUD System Owner[7], IT Project Manager, IT Program Manager, and/or Technical Point of Contact (TPOC) shall coordinate with the ISSO to create, submit, and monitor the RFC and associated POA&M. If necessary, the Chief Information Security Officer (CISO) is authorized to expedite the standard patching timeframes based on federal cybersecurity guidance for emerging vulnerabilities or security threats.

6.1 System, Utility and Application Patching

To the maximum extent possible, a regular schedule shall be employed for patching of all software, systems, and devices. In addition to security patching, patching includes updates to all enterprise operating systems and office productivity software, database software, third-party applications, and mobile devices under the direct management of the Infrastructure and Operations Office (IOO) or contractor application support staff. The RFC originator is responsible for supporting the testing required for each patch and proceeding with HUD's standardized Testing, Release, and Configuration Management requirements upon RFC approval.

Most vendors have automated patching procedures for their products or applications. There are many third-party tools to assist in the patching process and IOO uses the appropriate management software to support this process across the many different platforms and devices within HUD infrastructure. HUD system owners and associated staff responsible for external systems will ensure that support providers employ appropriate patch management tools as necessary for compliance. The regular application of

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

[5] Change impact analysis includes considerations related to cost, schedule, performance, training, information and implementation plan. Please refer to Appendix C for additional guidance.

[6] Plan of Action and Milestones (*POA&M*) is mandated by the Federal Information Systems Management Act of 2002 (FISMA) as a corrective action plan for tracking and planning the resolution of information security weaknesses.

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

critical security patches must be reviewed and tested as part of normal change management and audit procedures. Further, emergency, out-of-band security patches are applied within the schedule identified by issued DHS Emergency Directive guidance.

6.1.1 Patching of Personally Identifiable Information (PII) Systems

Patches for system components that store, transmit, process and/or receive PII, including, but not limited to, firmware, operating systems, databases and applications, must be applied using the standard maintenance schedule that complies with this policy.

HUD systems that contain PII are no longer eligible for a patch exception and must ensure the following:

a. Security patches for system components that store, transmit, process and/or receive PII (including, but not limited to, firmware, operating systems, databases and applications) must be applied in compliance with this policy.

b. Security patches must be tested prior to implementation and the test environment must comply with PII guidance[8], and

c. All system components on PII systems must be under current vendor support.

HUD systems that contain PII and have an existing POA&M and Risk-Based Decision (RDB) memo related to a DHS Emergency or critical patch exception must take the necessary capital planning steps to ensure resource are available to meet identified milestone timeframes. The capital planning steps include identification of the risk associated with patch management non-conformance and escalation as necessary.

6.1.2 End of Life Software

Vendors routinely stop supporting and releasing patches for older versions of their products and therefore, upgrades are required to retain the latest version that has on-going support. Software products no longer updated or patched by the manufacturer are considered end of life (EOL). All systems and associated components that contain PII must be under vendor support and patched to ensure compliance with this policy. Many vendors offer extended support programs for end-of-life products that allow access to previously released patches. The CCMB will only consider extended support programs by exception and these exceptions are requested using the Software Configuration Management (SCM) waiver template[9]. Any waiver for end-of-life products must provide a Risk-Based Decision (RBD) memo and POA&M to address non-compliance with this policy.

6.1.3 Patching Variance

Non-security patches may add new features to software and firmware, including security capabilities. New features may also be added through upgrades, which bring software or firmware to a newer version. Patches on production systems (e.g., servers and enterprise applications) may require complex testing and installation procedures. In certain non-security patching or upgrade cases, risk mitigation rather than patching and upgrading, may be preferable. The risk mitigation alternative selected should be determined through a risk assessment. The reason for any departure from the above standard and

[8] Guidance on the Protection of HUD Data; Chief Information Officer; December 12, 2019; http://hudatwork.hud.gov/HUD/cio/doc/dataguidance_121219

[9] SCM Waiver template is found on the CCMB website (http://hudatwork.hud.gov/HUD/cio/po/i/it/sd/devlife/def/CCMB/ccmb)

alternative protection measures taken shall be documented in writing (please refer to Section 10 Submitting a Request for Variance (RFV)). Variance from normal patch schedules all require written authorization from the Configuration Control Management Board.

6.2 Patch Management Guidance

Formal patch procedures shall be established to assess and prioritize patches based on the risk associated with the affected systems, that include:

- Impact to HUD data,
- Types of systems impacted
- Number of systems impacted
- Access level required to exploit the vulnerability being patched
- How extensive is the vulnerability exposure

Patch procedures also address testing patches to determine any impact to system components and confirm a systematic method for deployment. The patch implementation procedures for vulnerability and patch management shall ensure that application, system, and device vulnerabilities are:

- Evaluated regularly and responded to in a timely fashion
- Documented and well understood by support staff
- Automated and regularly monitored wherever possible
- Executed in a manner applicable vendor-supplied tools on a regularly communicated schedule
- Applied in a timely and orderly manner based on criticality and applicability of patches and enhancements

After a system patch has been deployed into production, the system is required to update current system configuration management documentation and prepare for future patches.

7 Roles and Responsibilities

a. Chief Technology Officer (CTO)

- Manages and oversees the configuration management (CM) program for HUD
- Monitors performance of the CM program and compliance with policies and procedures throughout system and product lifecycles

b. Configuration Control Management Board (CCMB)

- Establishes and reports on patch management performance
- Provides guidance on Patch Management policies and requirements
- Conduct reviews of Patch Management activities as required by the CM program verification and audit process and procedures
- Conduct final reviews of RFC information and associated feedback from the CISO and determines acceptability of submitted requests for variance to the patch management policy

c. Chief Information Security Officer (CISO)

- Disseminates federal guidance and information related to security patches to the the Office of Infrastructure and Operations (IOO), CTO/CCMB, ISSOs, and other appropriate parties for implementation planning/execution and awareness
- Coordinates with the Office of Infrastructure and Operations (IOO) and notifies the CTO / CCMB on critical patches requiring immediate release in HUD's infrastructure
- Notifies IT Project Managers and CTO/CCMB of critical patch requirements for external systems.
- Conducts initial reviews of RFCs and RFVs and associated impact analysis of patch requests proposed by the IOO for infrastructure systems and IT Project Managers for application systems.
- Submits RFC and RFV review feedback for approval/disapproval to the CCMB for final RFC and RFV determination.

d. Deputy CIO Infrastructure and Operations Office (IOO)

- Maintain and update operational patch management procedures for HUD's infrastructure to ensure patches are deployed in compliance with policy, within the required timeframes, adheres to organization security requirements and practices, and maximizes the confidentiality, availability, and integrity of information system component and functions.
- Notify the CTO/CCMB of all patch updates using the RFC template and confirms they are from an authorized source, relevant, virus free, and evaluated for patch prioritization and implementation.
- Test patches to determine any impacts to system components and confirm method to deploy security patches into production environment.
- Develop and maintain a regular schedule for the security patching of all software, systems, and devices, per this policy.
- For Non-commercial-off-the-shelf patches, the IOO shall establish the required timetable via a CVSS Base Rating.
- Request authority for variance using RFV template from the normal patch timeframes to the CISO for initial approval and then to the CCMB for final approval.
- Establish patch metrics for monitoring patch performance effectiveness and provide reports biannually to the CCMB[10].

e. RFC or RFV originator

- The RFC or RFV originator is the designated HUD System Owner, IT Project Manager, IT Program Manager, or Technical Point of Contact (TPOC) responsible for the system, application, or service.
- Notify the CCMB of all application patch updates using the RFC template and confirm they are from an authorized source, relevant, virus free, and evaluated for patch prioritization and implementation.

[10] NIST SP 800-40, Guide to Enterprise Patch Management Planning: Preventative Maintenance for Technology (Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology (nist.gov); Section 3.6 Choose Actionable Enterprise-Level Patching Metrics, April 2022.

- Notify and evaluate patches and associated impacts with the associated ISSO and create, submit, monitor, and report on the status of the RFC through the review, disposition, and implementation process.
- Ensure established patch management procedures and capabilities for applications that comply with patch management guidance.
- Coordinate with IOO on infrastructure patches that support their application, as well as the evaluation, testing, and implementation of application specific patches.
- Submit patch management SCM waiver requests or RFV for applications to CCMB for l approval.

8 Audit Controls and Management

Documented procedures and evidence of practice shall be in place for this operational policy as part of the configuration management policies and procedures. Examples of adequate controls include:

- System updates and patch logs for all major system and utility categories
- Information that verifies system ID, date patched, patch status, exception, and reason for the exception
- Demonstrated infrastructure enterprise patch management compliance across systems, applications, and devices via asset management tools and reports

9 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all employees at HUD. OITS evaluates compliance as part of security assessment and authorization (SA&A) process and continuous monitoring program. This includes enrollment of all systems in the Inventory of Automated System (IAS). The CCMB will conduct random internal audit assessments to verify compliance with this policy.

Any software or system found to be non-compliant shall require immediate corrective action. Where immediate corrective action is not possible, the ISSO and/or IT PM (as appropriate) must comply with the Plan of Action and Milestone Management Guide for remediation of IT system risk by creating a POA&M that is tracked in the CSAM system.

Repeated failures to follow this policy may lead to the removal of the software, system, or devices from the production environment, at the discretion of the Chief Information Officer. Staff members found in violation of this policy may be subject to disciplinary action, up to and including termination.

10 Submitting a Request for Variance

Request for variance (also known as exceptions or waivers) to the patch management policy require formal submission of the Request for Variance template and associated documentation for approval from the CCMB. A Request for Variance is considered a temporary departure from this policy. Each variance request must be accurate and complete to be considered by the CCMB.

Any approved software or hardware variance must provide an approved RBD and associated POA&M on file with the CCMB and the variance originator must provide status information on POA&M activities

11 Authorities and References

1. NIST Special Publication 800-40, Guide to Enterprise Patch Management Technologies
2. HUD Handbook 2400.25, Information Technology Security Policy
3. HUD Handbook 3252.1, Software Configuration Management Policy
4. HUD Handbook 3253.1, Change Management Policy
5. HUD Software Configuration Management (SCM) Procedures, Version 17, June 11, 2020
6. Public Law 114–210, the ‘‘Making Electronic Government Accountable By Yielding Tangible Efficiencies Act of 2016’’ or the ‘‘MEGABYTE Act of 2016,’’ July 29, 2016
7. OMB Memorandum M-16-12, Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing, June 2, 2016
8. Inventory of Automated Systems; http://intraportal.hud.gov/ias/
9. HUD Configuration Change Management Board; http://hudatwork.hud.gov/HUD/cio/po/i/it/sd/devlife/def/CCMB/ccmb
10. DHS / CISA Cybersecurity Directives; https://cyber.dhs.gov/directives/

12 Definitions

Selected terms used in Creating a Patch and Vulnerability Management Program are defined below.

Term	Definition
Application	Any data entry, update, query, or report program that processes data for the user.
Availability	Assurance that IT resources remain readily accessible to authorized users.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
End of Life	Any software program that is no longer supported by the manufacturer.
Exploit	A technique to breach the security of a network or information system in violation of security policy.
Firewall	A program that protects a computer or network from other networks by limiting and monitoring network communication.
Host	A computer or IT device (e.g., router, switch, gateway, firewall). The host is synonymous with the less formal definition of a system.
Integrity	Assurance that information retains its intended level of accuracy.
Operating System	The master control program that runs a computer.
Out-of-band Patch	An out-of-band patch is a patch released at some time other than the normal release time. The usual reason for the release of an out-of-band patch is the appearance of an unexpected, widespread, destructive exploit such as a virus, worm, or Trojan that will likely affect a large number of Internet users.
Patch	An additional piece of code developed to address a problem in an existing piece of software.
Remediation	The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, and uninstalling a software application.

Term	Definition
Risk	The probability that a particular threat will exploit a particular vulnerability.
System	A set of IT assets, processes, applications, and related resources that are under the same direct management and budgetary control; have the same function or mission objective; have essentially the same security needs, and reside in the same general operating environment. When not used in this formal sense, the term is synonymous with the term "host". The context surrounding this word should make the definition clear or else should specify which definition is being used.
System Owner	Individual with managerial, operational, technical, and often budgetary responsibility for all aspects of an information technology system.
Threat	Any circumstance or event, deliberate or unintentional, with the potential for causing harm to a system.
Trojan	A class of computer threats (malware) that appears to perform a desirable function but performs undisclosed malicious functions
Variance	A departure from an approved configuration, for a limited amount of time or for a specific product range, that does not require revision of the approved product baseline. Also known as a Waiver or Deviation.
Virus	A program designed with malicious intent that can spread to multiple computers or programs. Most viruses have a trigger mechanism that defines the conditions under which they will spread and deliver a malicious payload of some type.
Vulnerability	A flaw in the design or configuration of software has security implications. A variety of organizations maintain publicly accessible databases of vulnerabilities.
Worm	A type of malicious code particular to networked computers. It is a self-replicating program that works its way through a computer network exploiting vulnerable hosts, replicating, and causing whatever damage it was programmed to do.

13 Acronyms

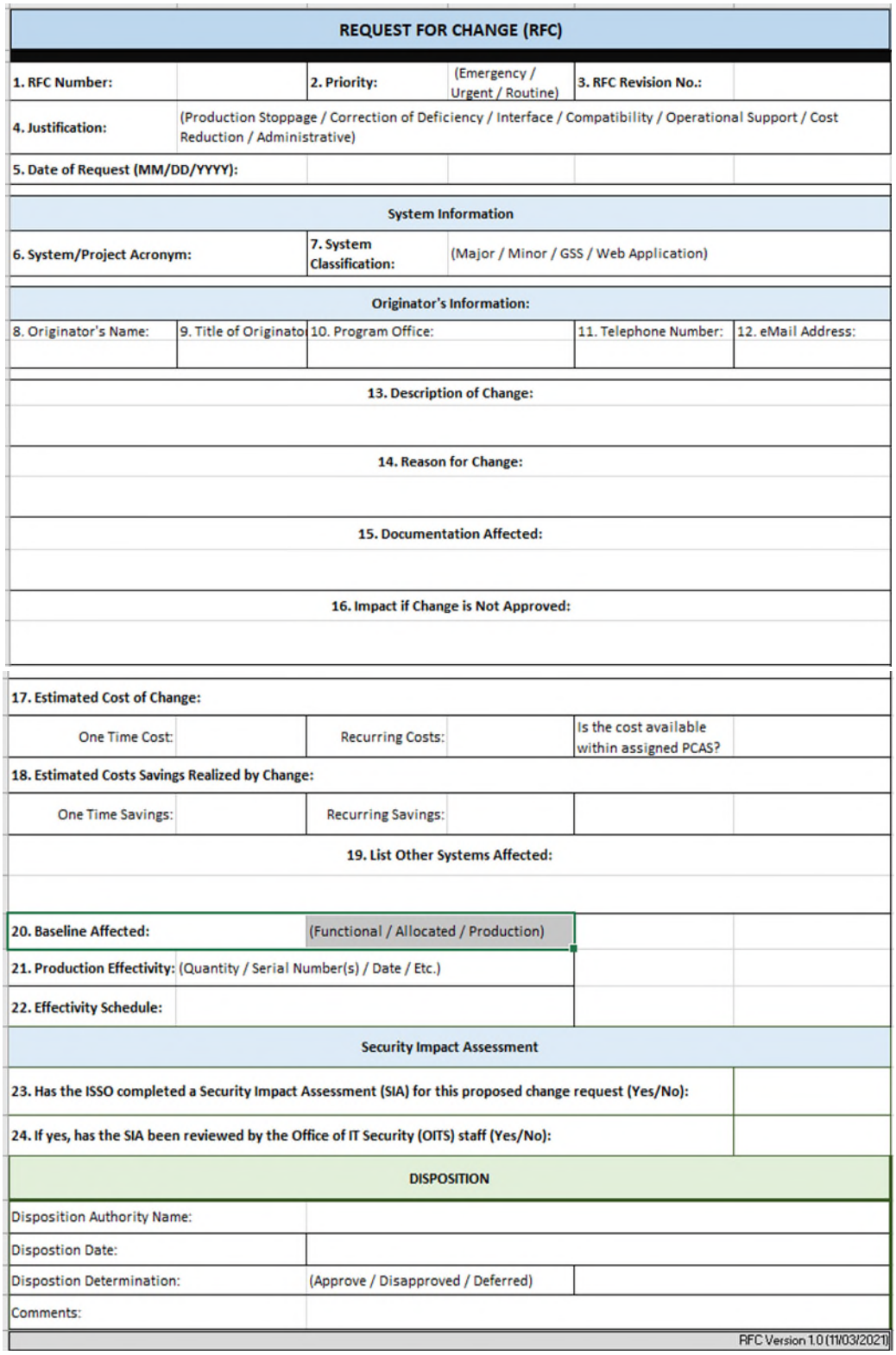
Acronym	Term
CCMB	Configuration Change Management Board
CISA	Cybersecurity and Infrastructure Security Agency
CSAM	Computer Security Assessment and Management
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
IAS	Inventory of Automated Systems
ISSO	Information System Security Officer
IT	Information Technology

IT PM	IT Project Manager
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
RBD	Risk Based Decision
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team

Appendix A Request for Change 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

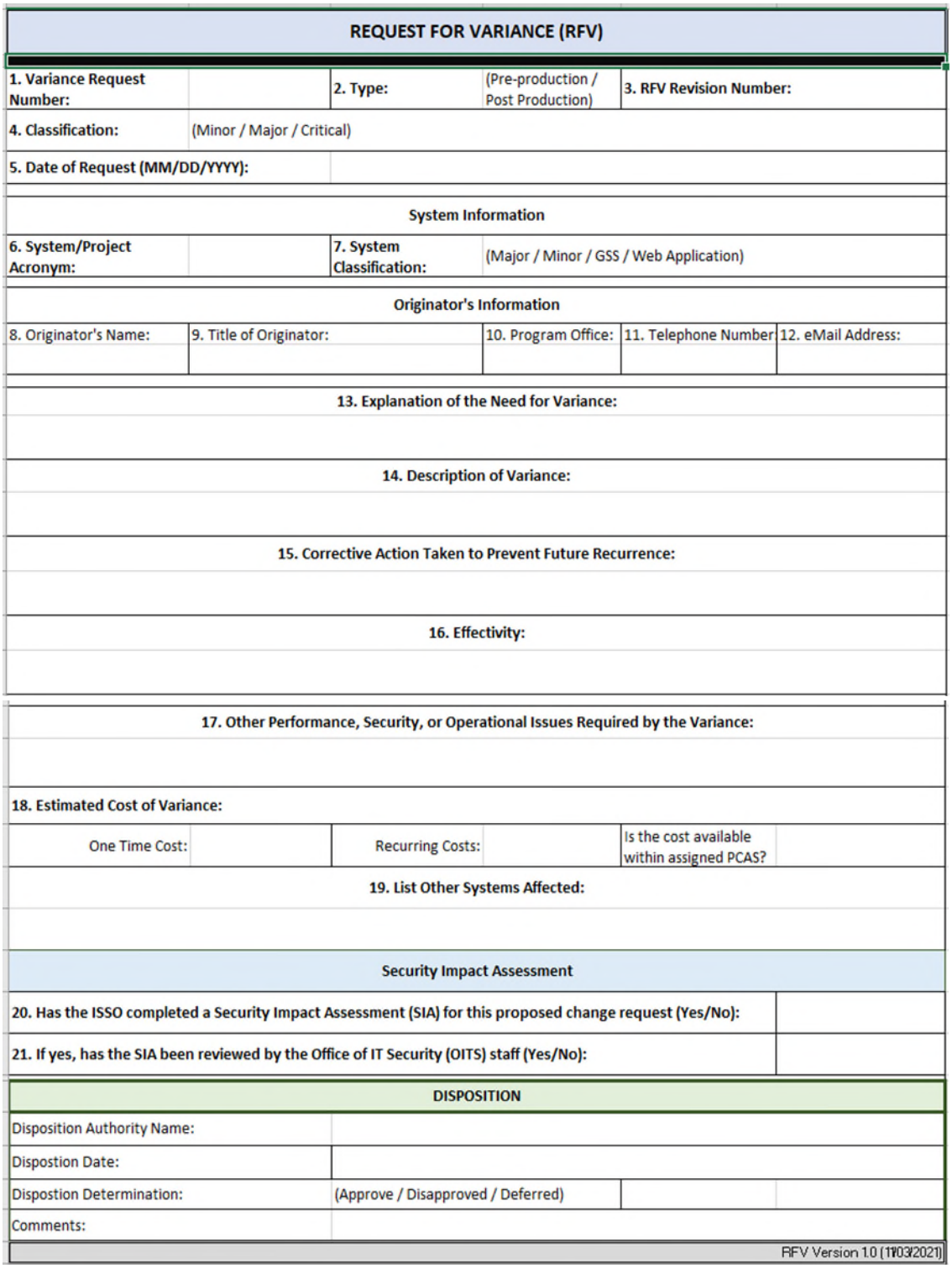


REQUEST FOR CHANGE (RFC)					
1. RFC Number:		2. Priority:	(Emergency / Urgent / Routine)	3. RFC Revision No.:	
4. Justification:	(Production Stoppage / Correction of Deficiency / Interface / Compatibility / Operational Support / Cost Reduction / Administrative)				
5. Date of Request (MM/DD/YYYY):					
System Information					
6. System/Project Acronym:		7. System Classification:	(Major / Minor / GSS / Web Application)		
Originator's Information:					
8. Originator's Name:	9. Title of Originato	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 Effectivity:	(Quantity / Serial Number(s) / Date / Etc.)				
22. Effectivity Schedule:					
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 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 Number	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:		Is the cost available within assigned PCAS?	
19. List Other Systems Affected:					
Security Impact Assessment					
20. Has the ISSO completed a Security Impact Assessment (SIA) for this proposed change request (Yes/No):					
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 Publicaton 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 patch.

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?