LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

HHS' Risk Based Decision Making

Check one or both as applicable:

New Request: ☑ Renewal: ☐

PURPOSE: The purpose of this Risk Based Decision (RBD) Request template and guidance is to formalize the management of known risks and to provide a mechanism to bring systems and processes into compliance with HHS Policies and Directives (applicable to Enterprise level systems needing HHS CISO approval and OpDiv level systems needing a pproval at the OpDiv level). This template is to serve as a tool for System Security or Privacy Officer (previously known as ISSO) and System Owners (SO) to document accepted risks associated with a system at any level. Not all sections in this template may apply depending on the request.

This RBD request template should be used to document and approve RBDs that are planned for any duration of time. For all RBDs, compensating controls to mitigate the risk must be documented and estimated time frames for completion provided.

APPROVAL: All HHS RBDs that impact HHS enterprise-wide systems and services, must be approved by the HHS Chief Information Security Officer (CISO). All other requests are approved by the OpDiv designated approval officials and do not require Departmental approval unless requested by the HHS CISO. Enterprise-wide systems/services refer to systems/services that are shared between the OpDivs and the Department or among two or more OpDivs. All RBDs must be reviewed at least **annually**. All OpDiv RBDs will be reported to the Department[1] on a monthly basis.

Route completed request through all designated stakeholders for review and approval as detailed within this template. The guidance and additional instructions in Appendix A will assist in the completion of this request.

Note: This template may be modified and used internally by OpDivs to document OpDiv system/ program-level RBDs. Complete all applicable sections.

Security Request: ☑ Privacy Request: ☐ **Internal Tracking Number (Optional):**

Domain:	☐ System Specific	☑ OpDiv-Wide		
	☐ Program Specific	☐ Enterprise-Wide		
Type of System [select all that apply]	☑ Financial System	☑ Contains PII	☑ High Value Asset	☐ Other

[1] The Department will have visibility into all RBDs through monthly reporting to the Governance, Risk, and Compliance division via the DeptGRC@hhs.gov email address.

Section 1: General Information				
Request Date (MM/DD/YY)	03/18/2025		OpDiv Name/Acronym	CMS
Requester Name/Title	Model Employee		Requestor Email/Phone Number	model.employee@cms.hhs.gov
System Name/Acronym or Policy Title	All CMS FISMA systems			
System UUID	n/a			
sGRC System ID				
System FIPS 199 Categorization	☑ High	☑ Moderate	☑ Low	☐ NA
NIST SP 800-30 Risk Rating	☐ High	☐ Moderate	☐ Low	☐ NA
System/Program Overview [Provide brief description of the system program and/or asset being impacted by this RBD request]	Pursuant to the March 2024 HHS Logical Access Memo, CMS would like to do a super secret and risky security thing that we need approval for.			
Requested Duration for RBD Request	Duration: 3 years		RBD Expiration Date: (MM/DD/YY) 03/03/2028	
	ATO Expiration Date: (MM/DD/YY)			
Requesting Organization	Program Area: CISO		System Owner Name:	
	System Security or Privacy Officer Name:			
Section 2: Policy Information				
Policy Directive/Statement [Identify the policy/section number (i.e., IS2P, Section 3.1.1a)]	HHS Approved Physical Access and Logical Access Authentication		If relevant, identify the NIST SP 800-53 control(s) applicable to this request	
State the policy as it appears in the HHS Policy Directive	HHS recognizes and accepts the following Multi Factor Authentication (MFA) logical access mechanisms: 1. Personal Identity Verification (PIV), to include derived credentials 2. Phishing-resistant MFA			
Section 3: RBD Information				
Deviation/Weakness Description/Plan of Action and Milestones (POA&M) information For RBD requests related to systems, identify the POA&M weakness number and brief description of POA&M or put "N/A" if no POA&M and provide a general Deviation/ Weakness description.	Weakness Description: We shouldn ' t train the AIs on the actual weaknesses.			
	Weakness Identifier: n/a			
	Scheduled Completion date: (MM/DD/YY)			

Risk Mitigation/ Compensating Controls Describe efforts to mitigate risk and document recommendation for management acceptance of residual risk. Describe the compensating controls in place. [Describe the actual risk(s) to the system/asset/ program and the compensating controls or other countermeasures either planned or implemented to mitigate risk]	The risk is that there is another set of credentials to possibly lose or break.
Operational and/or Mission Justification Describe the resulting impact if the RBD is approved/denied.	If this is approved, staff will find things even easier. If this is not aprroved, staff risk work stoppage.
Plan for Compliance Provide plan for bringing the system/program into compliance within specified duration time and state whether or not resources have been identified and are available to meet requirement. If a plan is not available, information must be included as to why this is not required.	This change is not a deficiency; it is adding another option to CMS ' s authentication options. This is adding compliance.
Additional Justification Provide the impact for accepting the risk, including PIA for impacted systems and/or other privacy documentation. [Additional documentation may be attached for further justification]	
Section 4: Privacy Impact Information	
Provide details on how PII or privacy is impacted.	There is not expected to be a direct impact to Privacy, as the authentication systems will still be using the right thing.
Attach privacy threshold analysis (PTA) or privacy impact assessment (PIA) for impacted systems and/or other privacy documentation.	

Section 5: Requesting Organization Signatures (System Specific Only)	
System Security or Privacy Officer	Name:
Signature:	Date: (MM/DD/YY)
System Owner (SO)	Name:
Signature:	Date: (MM/DD/YY)

Section 6: OpDiv Approvals			
1. OpDiv Program Director or Director Level Management	☐ Approved	☐ Approved with Conditions	☐ Denied
	☐ NA (no equivalent position)		
Name:			
Signature:	Date: (MM/DD/YY)		
Comments/Conditions:			
2, OpDiv Chief Financial Officer Note: Mandatory if it impacts a Financial System otherwise N/A	☐ Approved	☐ Approved with Conditions	☐ Denied
	☐ NA		
Name:			
Signature:	Date: (MM/DD/YY)		
Comments/Conditions:			

3. OpDiv Senior Official for Privacy	☐ Approved	☐ Approved with Conditions	☐ Denied
Name:			
Signature:		Date: (MM/DD/YY)	
Comments/Conditions:			
4. OpDiv Chief Information Security Officer (CISO)	☐ Approved	☐ Approved with Conditions	☐ Denied
Name:			
Signature:		Date: (MM/DD/YY)	
Comments/Conditions:			
5. OpDiv Authorizing Official (AO)	☐ Approved	☐ Approved with Conditions	☐ Denied
Name:			
Signature:		Date: (MM/DD/YY)	
Comments/Conditions:			
Date for Next Review if Approved:			

Section 7: HHS Approval			
NOTE: Only RBDs that impact enterprise-wide systems/services or those specifically requested by the Department are required to be approved by the HHS CISO. Submit the completed request THROUGH the OpDiv CISO, to the HHS Risk Management Program (securityriskmanagement@HHS.Gov) for the Department approval. If this is an urgent request, please note the urgency when submitting.			
HHS CISO	☐ Approved	☐ Approved with Conditions	☐ Denied
Name:			
Signature:	Date: (MM/DD/YY)		
Comments:			
Approval Conditions:			
If Approved, Date for Next Review: (MM/DD/YY)			
Reason/Comments if Denied:			

Appendix A: Guidance for Completing the RBD Request

The instructions below will assist in the completion of RBD requests and approval process.

I. Review/Renewal

All RBD requests must be reviewed annually and renewed every three (3) years if risk is not remediated/mitigated within 3 years since the initial approval or when significant changes are authorized, whichever comes first. Request must not exceed 3 years.

II. Risk-Based Decisions

RBDs are a mechanism to bring processes and systems into compliance with HHS Policies. A risk based decision includes all possible risk responses (accept, mitigate, transfer, avoid). Systems requiring acceptances involving findings, vulnerabilities and/or other deviations from security and privacy controls (e.g., audit finding, scan vulnerability, etc.) that cannot be remediated within a reasonable time period must have security controls, mitigations, and safe-guards in-place until the process/system can be brought into compliance with HHS Policy. SOs and AOs must sign and accept the risk from the RBD to ensure accountability through the RBD life-cycle.

Domain Definitions

Enterprise Wide – This refers to the HHS overall organization. If this box is checked, the RBD impacts HHS and/or multiple OpDivs (Source: Department).

OpDiv Wide – This refers to the OpDiv organization overall. If this box is checked, the RBD impacts a system that is utilized throughout multiple programs within the OpDiv. (Source: Department).

Program Specific – This refers to a particular program within the OpDiv (e.g., Human Resources, Grants, etc.) If this box is checked, the RBD impacts a specific program. (Source: Department).

System Specific – This refers to an information system and/or service. If this box is checked, the RBD impacts a specific information system or component(s) within an authorization boundary. (Source: Department).

III. System Definitions

Information System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.[2] (Source: 44 U.S.C., Sec. 3502; See also, HHS System Inventory Management Standard).

Financial System – System that contains cost and expenditures or other financial information regarding government purchasing, spending, or funding actions. (Source: Circular A-127, Financial Management Systems)

High Value Asset (HVA) System – A federal information system when associates to one or more of the following categories:

1. **Information Value** – the data the system processes, stores, or transmits is of high value to the Government and/or adversaries
2. **Mission Essential** – the owning agency cannot accomplish its mission essential functions within expected timeliness without that information system, and/or
3. **Federal Civilian Enterprise Essential** – the information system is designated as having a critical function of maintaining the security and resiliency of the Federal Civilian Enterprise. (Source: 0MB memorandum M-19-03)

[2] Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

System containing Personally Identifiable Information (PII) – PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (Source: OMB M-17-12, OMB Circular A-130)

Other System Types – Systems that do not directly apply to the above defined categories (Financial, HVA, or systems containing PII). (Source: Department)

IV. Section 1: Request/System Information

1. **When to Request an RBD:**

   OpDivs will request an RBD when OpDivs are unable to implement a Department policy (when unable to fully comply with all or any portion of the requirements of a Department Policy or Standard) OpDiv-wide or if the RBD impacts HHS enterprise-wide systems or solutions. OpDivs will document and have it approved by the Department. OpDivs are not required to obtain Department approval for a RBD if it only impacts OpDiv specific systems or components. Those RBDs are managed at the OpDiv level only.

2. **How to Complete the Request:**

   a. The information should be as complete as possible and N/A should only be used when there is no information that can be included.

   b. Multiple boxes may be selected as applicable from the section Type of Systems (this section is in the beginning of the request).

   c. In Section 1, under System/Program Overview field, should also include whether the RBD has OpDiv-wide impact and/or impacts enterprise-wide system or solution, and number of systems impacted by the RBD.

   d. In section 3, under Operational justification field, should also include compensating policy/security controls that are in place to mitigate risk.

   e. The attached request should be completed, signed and submitted to securityriskmanagement@hhs.gov

V. Section 2: Policy Information

1. Provide details on the Policy Directive/Statement for which an RBD is requested. If possible, link the NIST SP 800-53 control that is applicable.

VI. Section 3: RBD Information

1. **Document and Record RBD:**

   a. RBD requests must include documentation of operational mission impact risk acceptance, risk mitigation measures, and a POA&M for bringing the system procedures or control weakness into compliance, as applicable. The information in each section of this RBD template must be specific and include detailed concrete operational or mission focused reasons why the RBD should be approved. Depending on risk, the requests must be for an appropriate period based on a reasonable remediation strategy; however, they may not exceed three (3) years or ATO expiration (whichever comes first) without additional approval and should be reviewed on an annual basis to ensure the RBD is still justified.

   b. All HHS RBD requests sent to the Department are stored by HHS. Additionally, the OpDiv System Security or Privacy Officer is responsible for documenting any approved RBDs including accepted risks related to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (current version) security controls associated with an information technology (IT) system in the relevant System Security Plan (SSP) and tracked in the POA&M as part of the Security Assessment and Authorization (SA&A) process. The OpDiv System Security or Privacy Officer is also responsible for documenting any approved RBDs including accepted risks related to System Privacy Plans. The OpDiv System Security or Privacy Officer is responsible for submitting another RBD request, if required, upon expiration of the

existing RBD if the issue has not yet been resolved.

c. Any RBD request should be handled at the same risk classification level as the system to which it applies [low, moderate, high]. In addition, RBDs that include identification of system vulnerabilities and other sensitive information should be marked in compliance with applicable HHS Policy requirements.

2. **System program and/or asset being impacted**

   a. Provide brief description of the system program and/or asset being impacted by this RBD request.

   b. Provide duration of RBD request.

3. **Weakness Description & POA&M information**

   a. Identify the POA&M weakness number and brief description of POA&M.

   b. If this does not apply, enter "N/A" if no POA&M and provide a general weakness description.

   c. This information should reflect what has been documented in HSDW or an HHS/OpDiv tool.

4. **Describe efforts to mitigate risk and document recommendation for management acceptance of residual risk.**

   a. Describe compensating controls in place.

   b. Describe the actual risk(s) to the system/asset/program and the compensating controls or other countermeasures either planned or implemented to mitigate risk.

5. **Operational and/or Mission Justification/Impact**

   a. Describe the operational and/or mission justification/impact if the RBD is approved/denied.

6. **Compliance Plan**

   a. Provide a plan for bringing the system/program into compliance within the specified duration of time and state whether or not resources have been identified and are available to meet the requirement.

   b. If a plan is not available, information must be included as to why this is not required.

7. **Provide Additional Justification for Risk Acceptance**

   a. This may include cost, lack of resources, vendor, etc. and impact for accepting the risk.

   b. If additional documentation is needed, it may be attached to this RBD package for further justification.

VII. Section 4: RBD Privacy Impact Information

1. **Provide Impact that the Weakness Poses to Privacy Related Data.**

   a. Attach privacy threshold analysis (PTA) or privacy impact assessment (PIA) for impacted systems and/or other privacy documentation.

   b. Provide details on how personally identifiable information (PII) or privacy is impacted.

VIII. Section 5: Requesting Organization Signatures (System Specific Only)

1. Written authorization (via dated signature on the request form) from the OpDiv's System Security or Privacy Officer and System Owner (SO) are required to submit a request.

IX. Section 6: OpDiv Approvals

1. All RBD requests that impact Departmental policy or standard that has OpDiv-wide impact and/or impacts enterprise-wide systems or solutions must be approved by the HHS CISO. All other requests require OpDiv approval only.

2. Any RBD requests for Designated Financial Systems must be submitted to and approved by the OpDiv's CFO prior to submission to the HHS CISO. Any privacy RBD must be submitted to and approved by the OpDiv Senior Official for Privacy (SOP). All requests must be coordinated with the OpDiv Authorizing Official (AO) prior to submission.

X. Section 7: HHS Approval

1. All policy RBDs that have an enterprise-wide impact, must be approved by the HHS CISO.

    a. Submit policy RBD requests to the securityriskmanagement@hhs.gov mailbox for Department approval. The requests are entered into the review queue to begin the approval process. The RBD request is not approved until returned with the HHS CISO signature.

    b. If the RBD request is not approved, the form detailing the reasons is returned to the OpDiv.