Homeland Security

DHS 4300A

Information Technology System Security Program, Sensitive Systems

Attachment B

Information System Waiver and Risk Acceptance Requests

Version 1.0

July 30, 2022

Document Change History

Version	Date	Description
1.0	July 30, 2022	Updated Processes and authorities and changed form for waiver and risk acceptance requests (Update by CISOD Office of Compliance

Contents

Request for Information System Waiver or Risk Acceptance

1.0 INTRODUCTION

This procedure is a requirement of DHS Sensitive Systems Policy Directive 4300A, (CA) Assessment, Authorization, and Monitoring Control Family Section 4 through 6.

For additional information on waiver and risk acceptances, refer to DHS 4300A,"Information Technology System Security Program, Sensitive Systems" Attachment H.

Form shall be used when requesting a waiver or risk acceptance for an Information System (IS) security weakness. A weakness is any information security vulnerability that could compromise the confidentiality, integrity, or availability of an IS. Review Section 2.0, "Instructions" before starting the form.

Requests should be handled at the -security classification level as the system to which the identified weakness applies and must be appropriately marked. For an Unclassified waiver or risk acceptance that includes the identification of system vulnerabilities, the request should be marked "For Official Use Only."

As per 4300A Attachment H, Section 3.20 and 3.21, waivers and risk acceptance request forms shall be used:

1. A waiver request may be submitted when a system or program is unable to fully comply with any

portion of this Directive. A waiver does not bring the system or program into compliance with policy. It is an acknowledgement by the Component CISO of non-compliance with policy and that compensating controls have been implemented and an acceptable plan is in place to remediate the weakness.

Waiver requests are routed through the System Owner, Program Manager, ISSO, ISSM, Authorizing Official, and submitted to the Component's CISO for final approval. All submitters coordinate with the Authorizing Official (AO) prior to submission to the Component CISO.

Exceptions are any vulnerability, or finding, that impacts DHS Critical Controls, Executive Directives, Binding Operational Directives, or Emergency Orders, etc.

2. A Risk Acceptance request may be submitted when a system or program identifies a weakness where no viable remediation is available. Compensating Controls must be implemented.

Risk Acceptance requests are routed through the System Owner, Program Manager, ISSO, ISSM, Component CISO, and submitted to the Component AO. The AO may decide to accept the risk at their discretion.

CFO Designated Systems: Waiver and risk acceptance requests for CFO-designated systems must include the Component's Chief Financial Officer (CFO) approval.

Privacy Sensitive Systems: Waiver and risk acceptance requests for systems designated by the Privacy Office as privacy sensitive systems must include the Component Privacy Officer or Senior Privacy Point of Contact (PPOC) approval.

Enterprise, Mission Essential System, and High Value Assets: Waiver and risk acceptance requests for these systems and programs must be routed to the DHS CISO for approval.

Request for Information System Waiver or Risk Acceptance

2.0 INSTRUCTIONS

Most form fields are self-explanatory, but specific instructions will ensure key information is provided to determine a waiver or risk acceptance using a risk-based approach.

1. DHS Tracking Number will be entered by the Waiver Team at DHS CISOD.
2. Limit responses to the form fields. If additional space is needed, use the continuation space in Section V; for each continued item, identify the name of the field being continued. Start a new paragraph for each continued item.
3. For "Requested waiver length," enter a number of months from 1 to 12.
4. Risk Acceptances do not have an expiration date but shall be reviewed at least annually to ensure the risk remains acceptable and updated as needed.
5. There is no ATO expiration date for OA systems.
6. In Section II of the form, Provide the 4300A policy statement number(s), associated NIST SP 800-53 control(s), audit/finding number, and/or description of any vulnerability/weakness applicable to this request. If more than one "pair," separate them with semicolons.
7. With respect to CFO and Privacy review and approval, either may be given before the other.
8. When signing the form, digital signatures are preferred. Do not lock the document; locked forms will be rejected.
9. Ensure that the form is forwarded for approval to the Component CFO and/or Senior PPOC if required. Supporting documentation should be attached to the submission. Examples include project plans, diagrams, supporting evidence/artifacts.
10. Ensure that all Component-level approvals are completed for the waiver or risk acceptance request. Requests that are incomplete as to approvals will not be processed.
11. Submit the form using the DHS Component defined process.
12. The CISOD Policy Team will add the DHS tracking number upon receipt and include the tracking numbers in its acknowledgment of receipt.

Address questions and concerns to infosecpolicy@hq.dhs.gov.

Request for Information System Waiver or Risk Acceptance

DHS Tracking Number: Component Tracking Number:

SECTION I: SYSTEM INFORMATION

Date: Component:

IACS System Name:

IACS System ID:

ATO Expiration Date: In Ongoing Authorization (OA) Program: Yes No

Select System Designation: CFO System Privacy System MES HVA Enterprise

Select Request Type: Waiver Risk Acceptance

Provide a brief description of the system for which the waiver/risk acceptance is requested (e.g., financial system, accounting), describe the system architecture; attach a diagram if available. This information is generally found in the System Security Plan:

SECTION II: WAIVER/RISK ACCEPTANCE INFORMATION

Provide the 4300A policy statement number(s), associated NIST SP 800-53 control(s), audit/finding number, and/or description of any vulnerability/weakness applicable to this request:

Provide description of weakness or issue identified above:

Justification for request. Describe the factors prohibiting remediation of the weakness and why the waiver or risk acceptance is needed (e.g. lack of funding, technology unavailable, vendor patch unavailable):

Describe the compensating controls implemented to mitigate risk:

Describe system or program stakeholders' remediation or project plan:

Request for Information System Waiver or Risk Acceptance

DHS Tracking Number | Component Tracking Number

SECTION III: PLAN OF ACTION AND MILESTONES

Describe or attach the Plan of Action and Milestones (POA&M):

POA&M Number(s):

POA&M scheduled completion date:

Is this a renewal of an existing POA&M Waiver or Risk Acceptance? Yes ☐ No ☐

POA&M original scheduled completion date:

SECTION IV: APPROVALS

Requestor

Requestor Name:

Date:

Requestor signature

System Owner

System Owner Name:

Recommend approval ☐

Do not recommend approval ☐

Date:

System Owner signature

Component CISO

Component CISO Name:

Recommend approval ☐

Do not recommend approval ☐

Date:

Component CISO signature

Authorizing Official

Authorizing Official Name:

Recommend approval ☐

Do not recommend approval ☐

Date:

AO signature

Requested waiver length (in months) or expiration date:

For risk acceptances: **I accept the risk described in this risk acceptance document.** ☐

Request for Information System Waiver or Risk Acceptance

DHS Tracking Number | Component Tracking Number

SECTION IV: APPROVALS (CONT'D)

Component CIO *(signature not required when CIO is the AO)*

Component CIO Name:
Recommend Approval
Do not recommend approval
Date:

Component CIO signature

Component CFO

Is this a CFO-designated system? Yes No
Component CFO Name:
Recommend Approval
Do not recommend approval
Date:

CFO signature (if applicable)

Component Privacy

Is this a Privacy system? Yes No
Component Priv. Official Name:
Recommend Approval
Do not recommend approval
Date:

Privacy Official signature (if applicable)

DHS CISO or Deputy CISO *(Note: The DHS CISO must approve waivers and risk acceptances that impact DHS enterprise systems, MES, HVAs, or DHS HQ systems):*

Approved
Expiration date:
Conditions for approval:

Disapproved
Reasons for disapproval:

CISO or Deputy CISO

Name:
Title:
Date:

Request for Information System Waiver or Risk Acceptance

DHS Tracking Number | Component Tracking Number

SECTION V: ITEM CONTINUATIONS IF NEEDED. (SEE INSTRUCTIONS).