Homeland Security

DHS 4300A

Sensitive Systems Handbook

Attachment B

Waiver Request Form

Version 11.0

July 30, 2014

Protecting the Information that Secures the Homeland

Document Change History

Version	Date	Description
2.0	March 31, 2004	Initial release
2.1	July 26, 2004	Development of form
3.0	July 29, 2005	Minor editorial changes
4.0	June 1, 2006	No change
5.0	March 1, 2007	No change
6.0	May 14, 2008	Section 1.0 Updated Introduction text to specify that the form shall only be submitted by the Component Information Systems Security Officer (CISO) or the Component Information Systems Security Manager (ISSM). Request Form Updated to include TAF System Name, TAF Inventory ID, System Owner Name, POA&M Weakness Number, and Scheduled Remediation Completion Date, and Identificaiton of 800-53 controls.
6.1	September 23, 2008	Section 1.0 Updated Introduction text to specify that the form shall only be submitted by the “Component Information Systems Security Officer

		(CISO)/Information Systems Security Manager (ISSM)." Request Form Changed "IT Security Policy" to "Information Security Policy."
6.1.1	April 23, 2009	Request Form Updated form to include Component Tracking Numbers.
7.0	August 7, 2009	Section 1.0 Introduced new terminology Authorizing Official (AO) – replaces DAA, as per NIST 800-37 and 800-53
7.1	June 21, 2010	Section 1.0 Updated to remove the stipulation that only waivers and exceptions for key controls must go to the CFO or Chief Privacy Officer first. Request Form Includes signature fields for Component Chief Financial Officer and Component Senior Privacy Official.
9.1	July 24, 2012	New request form design.
11.0	July 30, 2014	Revised form to remove exception requests.

INTRODUCTION

When requesting a waiver to the DHS Sensitive Systems Policy Directive 4300A, the attached form is to be filled out electronically and submitted as a PDF file. Section 1.5 of the DHS 4300A Sensitive Systems Handbook provides additional guidance regarding the request of waivers.

Any waiver request should be handled at the same classification level as the system to which it applies, either unclassified or classified. For an unclassified waiver that includes the identification of system vulnerabilities, the request should be marked "For Official Use Only."

Waiver request forms shall only be submitted by the Component Chief Information Systems Security Officer (CISO) or Information Systems Security Manager (ISSM).

Any waiver requests for CFO designated Systems must additionally be submitted to the Component's CFO for approval before submitting to the DHS CISO.

Any waiver requests for systems designated by the Privacy Office as Privacy Sensitive Systems must additionally be submitted to the Component's Privacy Officer or Senior Privacy Point of Contact (PPOC) for approval before submitting to the DHS CISO.

Submit the completed form through the Component CISO or ISSM, for forwarding to the DHS CISO, via the IT Security Policy mailbox at infosecpolicy@hq.dhs.gov. When waiver forms are received at the infosecpolicy@hq.dhs.gov address, they are entered into the approval queue to begin the approval process.

Homeland Security

Information Security Program

Request for Waivers

System Information	
Date:	DHS Tracking Number:
Component:	Component Tracking Number:
IACS System Name:	IACS System ID:

Approvals		
System Owner Name: Recommend approval ☐ Do not recommend approval ☐	System Owner Signature: Date:	
Requestor Name: Recommend approval ☐ Do not recommend approval ☐	Requestor Signature: Date:	
Authorizing Official Name: Recommend approval ☐ Do not recommend approval ☐	Authorizing Official Signature: Date:	
Component CISO Name: Recommend approval ☐ Do not recommend approval ☐	Component CISO Signature: Date:	
Financial System? ☐	Component CFO Name: Recommend approval ☐ Do not recommend approval ☐	Component CFO Signature: Date:
Privacy Sensitive System? ☐	Component Chief Privacy Officer Name: Recommend approval ☐ Do not recommend approval ☐	Component Chief Privacy Officer Signature: Date:

Waiver Information

Identify Policy Directive statement by section number (including letter if any; for example, 3.1.1.a):
State the policy as it appears in the DHS Policy Directive:
If relevant, identify the NIST SP 800-53 control(s) applicable to this request:
Provide a brief description of the system for which the waiver is requested:
Describe the operational and mission impact of the current policy:
Describe efforts to mitigate risk introduced, and management acceptance of residual risk, if the waiver is approved:
Provide a security plan for bringing the system into policy compliance within the waiver's validity period, and state whether or not resources have been identified and are available to meet requirement:
Provide any additional justification for the waiver request:
Provide the length of time for which the waiver is requested:
For existing systems, identify the POA&M weakness number that identifies the system or program remediation plan that will bring the system back into compliance: POA&M Weakness Number: Scheduled completion date:
Submit the completed form through the Component CISO or ISSM, for forwarding to the DHS CISO, via the IT Security Policy mailbox at infosecpolicy@hq.dhs.gov.

DHS CISO Name:	DHS CISO Signature: Date:
☐ Approved for month waiver	☐ Disapproved
Conditions for approval:	
Reason if disapproved:	