U.S. Customs and
Border Protection

Attachment B

Waivers and Exceptions Request Form

HB 1400-05D

Information Systems Security Policies and Procedures Handbook

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	July 27, 2009	Initial CBP 1400-05D release based solely on DHS 4300A, Version 6.1.1, attachment. There are no substantive differences between this CBP attachment and its source DHS attachment. This attachment is included as part of the CBP 1400-05D handbook suite to enable the CBP user to be able to access all IT security policies (DHS as well as CBP specific) at one location.
2.0	December 21, 2010	Updates reflecting changes from DHS in Section 1.0 removing stipulation that only waivers and exceptions for key controls must go to the CFO or Chief Privacy Officer first. Also formally updated the template to include signature lines for the Chief Privacy Officer and the Chief Financial Officer.

1.0 INTRODUCTION

When requesting a waiver or exception to DHS IT security policy, the following form is to be used, filled out electronically and saved as a Microsoft Word file. DHS 4300 Section 1.5 of this document provides additional guidance regarding the request of waivers and exceptions.

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

Waiver and Exception Request forms shall only be submitted by the CBP Information Systems Security Officer (CISO).

Any waiver or exception requests for Chief Financial Officer (CFO) designated Systems must additionally be submitted to the Component's CFO for approval before submitting to the DHS CISO.

Any waiver or exception requests of a key control for Privacy Office designated 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 CISO/ISSM completed form to the DHS Chief Information Security Officer (CISO), or forms can be e-mailed to the Director for IT Security Policy at INFOSEC@dhs.gov. When Waiver and Exception forms are received at the INFOSEC@dhs.gov address, they are entered into the approval queue to begin the approval process.

DHS Information Security Program
Waivers and Exceptions Request

Date: _____ **Request Tracking Number:** _____

(To be filled in by DHS CISO staff)

Component Name: Customs and Border Protection

TAF System Name: _________________ **TAF Inventory ID:** _________________

System Owner Name: _________________ **E-mail address:** _________________

Telephone: _________________

DAA Name: _________________ **E-mail address:** _________________

Requestor Name: _______________________ **E-mail address:** _________________

Component CISO / ISSM

CFO Designated System □

CBP Chief Financial Officer Name: _________________ **Received CFO Approval:** □

Privacy Office Designated System □

CBP Senior Privacy Official Name: _________________ **Received Privacy Approval:** □

Type of request:

□ Waiver □ Second Waiver □ Exception

Requesting waiver/exception from:

□ *DHS Sensitive Systems Policy 4300A* □ *DHS National Security Systems Policy 4300B*

Identify policy by section number and letter within the DHS policy directive (e.g., 3.1.1.a): _____

State the policy as it appears in the DHS policy directive: _____

Describe the operational and mission impact of the current policy: _____

If relevant identify the 800-53 Control(s) applicable to the waiver or exception request:

Describe efforts to mitigate risk introduced, and management acceptance of residual risk, if the waiver/exception is approved: _____

For waiver requests, provide security plan for how the situation will be brought back to policy compliance within six months and if resources have been identified and are available to meet requirement: _____

Provide any additional justification for the waiver/exception request: _____

For waiver requests to existing systems, identify the POA&M weakness number, which identifies the system or program remediation plan to bring the identified system back into compliance.

POA&M Weakness Number: __________   Scheduled Completion Date: ________

<u>Submit completed form through the Component Information Security Officer (CISO)/Information Systems Security Manager (ISSM)</u> to the DHS Chief Information Security Officer (CISO). For expedited consideration while awaiting ISSM/CISO signature, also e-mail completed form to the Director for Information Security Policy at INFOSEC@dhs.gov.

DHS CISO Signature   Date:

□ Disapproved   □ Approved

Reason if disapproved: _________________________