DHS 4300A, “Information Technology System Security Program, Sensitive Systems”

Attachment P

Policy Change Requests

Version 12.0

August 5, 2022

Protecting the Information that Secures the Homeland

Document Change History

Version	Date	Description
2.0	March 31, 2004	Initial release
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	No change
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."
7.0	August 7, 2009	No change
9.1	July 24, 2012	Edited for spelling and grammar. Change Request form redesigned
11.0	August 5, 2014	.Email address for reporting changed to INFOSEC@HQ.DHS.GOV. Request Form no longer allows requests for National Security Systems documents (4300B series).
12.0	August 5, 2022	Added procedures for CISO Council review and approval for all DHS Cybersecurity policy change requests. Added role for Policy Working Group.

Introduction

This Attachment to the Department of Homeland Security (DHS) 4300A contains the change request form and procedures to use for requesting changes to any DHS cybersecurity policy document. The forms should be emailed to the DHS Director of Cybersecurity Policy at infosecpolicy@hq.dhs.gov.

CHANGE REQUEST PROCESS

Requested changes to DHS cybersecurity policies shall be submitted to the DHS Director of Cybersecurity Policy at infosecpolicy@hq.dhs.gov for review, and evaluation utilizing the below form. The Policy Working Group, consisting of the Headquarters (HQ) DHS Policy Team, and representatives from the components, will provide the initial evaluation of the request, along with any Subject Matter Expert (SME) input, if necessary.

Policy change requests should be submitted by the component CISO but may also come from other stakeholders such as the component Privacy Officer, CFO, CPO, or CSO. In addition, the CISO Council may task the Policy Working Group to evaluate a particular area of policy and make recommendations for change to the Council.

After initial evaluation, the Policy Working Group will present the change recommendation to the DHS CISO Council for consideration. Requested changes must be approved by a majority of the voting members from the CISO Council.

Requested changes to cybersecurity policy will be presented to the CISO Council on a routine basis, as they are submitted for evaluation by the Policy Working Group. Emergent changes will also be presented to the CISO Council as necessary, to reflect any new or updated cybersecurity laws, Executive Orders, directives, threats, or vulnerabilities, etc., that will have an effect on the operating environment. In addition, the Policy Working Group will present an annual status update on DHS cybersecurity policy, with any necessary updates or revisions, to the CISO Council for consideration and approval. The Policy Working Group will conduct an annual review of DHS cybersecurity policy and present the findings in its annual policy status update to the CISO Council. This will reflect any recommended changes from new or revised cybersecurity laws, Executive Orders, or directives, that haven't already been captured through ad hoc recommendations and updates.

DHS IT Security Program

Document Change Request

Date:

Tracking Number:

(To be filled in by DHS staff)

From (name):

Component:

Telephone Number:

Email address:

Policy or document for which change is requested (include version number if applicable):

Section/paragraph affected:

Description of issue or problem:

Suggested change or modification (include the suggested text):

Justification for the change request:

Tracking Number:

Suggested change reviewed by (name):

CISO Council Presentation Date:

Decision:

☐ Approved

☐ Disapproved. Reason for disapproval:

Director of Cybersecurity Policy

(For approved changes): **Change included in document Version** **dated**

Email completed form to the Cybersecurity Policy Branch at infosecpolicy@hq.dhs.gov.