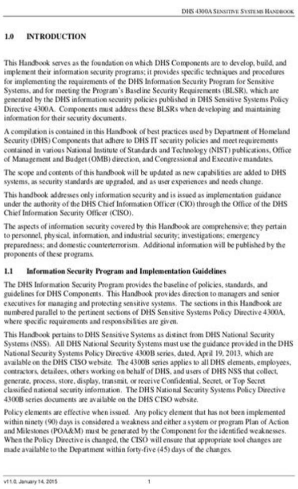

DHS 4300A SENSITIVE SYSTEMS HANDBOOK

1.0 INTRODUCTION

This Handbook serves as the foundation on which DHS Components are to develop, build, and implement their information security programs; it provides specific techniques and procedures for implementing the requirements of the DHS Information Security Program for Sensitive Systems, and for meeting the Program's Baseline Security Requirements (BLSR), which are generated by the DHS information security policies published in DHS Sensitive Systems Policy Directive 4300A. Components must address these BLSRs when developing and maintaining information for their security documents.

A compilation is contained in this Handbook of best practices used by Department of Homeland Security (DHS) Components that adhere to DHS IT security policies and meet requirements contained in various National Institute of Standards and Technology (NIST) publications, Office of Management and Budget (OMB) direction, and Congressional and Executive mandates.

The scope and contents of this handbook will be updated as new capabilities are added to DHS systems, as security standards are upgraded, and as user experiences and needs change.

This handbook addresses only information security and is issued as implementation guidance under the authority of the DHS Chief Information Officer (CIO) through the Office of the DHS Chief Information Security Officer (CISO).

The aspects of information security covered by this Handbook are comprehensive; they pertain to personnel, physical, information, and industrial security; investigations; emergency preparedness; and domestic counterterrorism. Additional information will be published by the proponents of these programs.

1.1 Information Security Program and Implementation Guidelines

The DHS Information Security Program provides the baseline of policies, standards, and guidelines for DHS Components. This Handbook provides direction to managers and senior executives for managing and protecting sensitive systems. The sections in this Handbook are numbered parallel to the pertinent sections of DHS Sensitive Systems Policy Directive 4300A, where specific requirements and responsibilities are given.

This Handbook pertains to DHS Sensitive Systems as distinct from DHS National Security Systems (NSS). All DHS National Security Systems must use the guidance provided in the DHS National Security Systems Policy Directive 4300B series, dated, April 19, 2013, which are available on the DHS CISO website. The 4300B series applies to all DHS elements, employees, contractors, detailees, others working on behalf of DHS, and users of DHS NSS that collect, generate, process, store, display, transmit, or receive Confidential, Secret, or Top Secret classified national security information. The DHS National Security Systems Policy Directive 4300B series documents are available on the DHS CISO website.

Policy elements are effective when issued. Any policy element that has not been implemented within ninety (90) days is considered a weakness and either a system or program Plan of Action and Milestones (POA&M) must be generated by the Component for the identified weaknesses. When the Policy Directive is changed, the CISO will ensure that appropriate tool changes are made available to the Department within forty-five (45) days of the changes.

v11.0, January 14, 2015 1