

UNCLASSIFIED



# **TRADITIONAL SECURITY CHECKLIST OVERVIEW**

**Version 2, Release 5**

**24 January 2024**

**Developed by DISA for the DOD**

UNCLASSIFIED

### **Trademark Information**

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
<b>1. INTRODUCTION .....</b>	<b>1</b>
1.1 Executive Summary.....	1
1.2 Authority.....	1
1.3 Vulnerability Severity Category Code Definitions .....	1
1.4 Checklist Distribution.....	2
1.5 Document Revisions .....	2
1.6 Other Considerations .....	2
1.7 Product Approval Disclaimer .....	2

## 1. INTRODUCTION

### 1.1 Executive Summary

The Traditional Security Checklist is published as a tool to provide and improve upon the minimum requirements for the security of Department of Defense (DOD) facilities that house DISN (unclassified/classified) assets. This document is intended to be used while conducting Command Cyber Readiness Inspections (CCRI), System Assessment and Authorization (A&A), unit self-inspections as a reference guide for addressing physical security requirements for owners of facilities housing IA systems.

### 1.2 Authority

This checklist overview is composed of several volumes, each containing its own purpose. The purpose of the overview, as authorized by DOD Directive (DODD) 5143.01 (Reference (a)) and DOD Instruction (DODI) 5200.01 (Reference (b)), is to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP). This guidance is developed in accordance with Reference (b), Executive Order (E.O.) 13526, E.O. 13556, and part 2001 of title 32, Code of Federal Regulations (CFR) (References (d), (e), and (f)). This combined guidance is known as the DOD Information Security Program. This overview is also published in accordance with the authority contained in DOD Regulation 5200.08-R, Physical Security Program, April 2007; DOD Manual 5200.01-M, Volume 3, DOD Information Security Program: Protection of Classified Information, 24 February 2012 and DOD Manual 5200.02, Procedures for the Personnel Security Program, 3 April 2017. This Instruction also derives limited authority from Committee on National Security Systems Instruction (CNSSI) 7003, Protected Distribution System (PDS), September 2015. Although the use of the principles and guidelines in this STIG provides an environment that contributes to the security requirements of DOD facilities and systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures.

### 1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

Category	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will <b>directly and immediately</b> result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which <b>has a potential</b> to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which <b>degrades measures</b> to protect against loss of Confidentiality, Availability, or Integrity.

## 1.4 Checklist Distribution

Parties within the DOD and federal government's computing environments can obtain the Traditional Security Checklist from the DOD Cyber Exchange website at <https://cyber.mil/>. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the checklist from <https://public.cyber.mil/>.

## 1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: [disa.stig\\_spt@mail.mil](mailto:disa.stig_spt@mail.mil). DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

## 1.6 Other Considerations

DISA accepts no liability when applying specific requirements for the security of DISN assets on the basis of the Traditional Security STIG checklist. There are a variety of environments, and each organization must take that into consideration when applying the Traditional Security STIG checklist. These are the minimum requirements for securing DISN assets.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied correctly

## 1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

The Traditional Security STIG provides minimum operational security guidance for the security of DOD/DISN assets. The STIG, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports command cyber readiness inspections (CCRI) and system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a

product that has a STIG for product evaluation and RMF purposes from [disa.stig\\_spt@mail.mil](mailto:disa.stig_spt@mail.mil). This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (<https://www.niap-ccevs.org/>) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (<https://csrc.nist.gov/groups/STM/cmvp/>) IAW Federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (<https://www.disa.mil/network-services/ucco>) IAW DODI 8100.04.