

Build and Operate a Trusted DoDIN

ORGANIZE											
Lead and Govern											
2022 National Security Strategy	2022 National Defense Strategy (NDS)	National Military Strategy (NMS)	2019 National Intelligence Strategy	2023 National Cybersecurity Strategy	National Cybersecurity Strategy Implementation Plan	National Strategy to Secure 5G	U.S. Int'l Strategy for Cyberspace	NIST Cybersecurity Framework	CISA Cybersecurity Strategic Plan	National Cyber Workforce and Education Strategy	United States Intelligence Community Information Sharing Strategy
2022 DoD Zero Trust Strategy	2023 DoD Cyber Strategy (Fact Sheet)	DoD Cyber Workforce Strategy	DoD Digital Modernization Strategy	DoD Artificial Intelligence Strategy (unclass summary)	DoD OCONUS Cloud Strategy	DoD Data Strategy	DoD Identity, Credential, and Access Management (ICAM) Strategy	DoD 5G Strategy	DoD Software Modernization Strategy	DoD Information Security Continuous Monitoring (ISCM) Strategy	DoD Cybersecurity Reference Architecture (Version 5.0)

ORGANIZE
Design for the Fight
NIST SP 800-119 Guidelines for the Secure Deployment of IPv6
CNSS National Secret Fabric Architecture Recommendations
DoDD 5000.01 Defense Acquisition Framework
DoDD 5200.47E Anti-Tamper (AT)
DoDD 8115.01 IT Portfolio Management
DoDI 5000.82 Requirements for the Acquisition of Digital Capabilities
DoDI 5200.44 Protection of Mission Critical Functions to Achieve TSN
DoDI 8115.02 IT Portfolio Management Implementation
DoDI 8330.01 Interoperability of IT and National Security Systems (NSS)
DoDI 8580.1 Information Assurance (IA) in the Defense Acquisition System
DODAF (Version 2.02) DoD Architecture Framework
CJCSI 5123.01 Charter of the JROC and Implementation of the JCIDS

ENABLE
Secure Data in Transit
FIPS 140-3 Security Requirements for Cryptographic Modules
CNSSP-1 National Policy for Safeguarding and Control of COMSEC Material
CNSSP-17 Policy on Wireless Communications: Protecting Nat'l Security Info
CNSSP-25 National Policy for PKI in National Security Systems
NACSI-2005 Communications Security (COMSEC) End Item Modification
CNSSI-5001 Type-Acceptance Program for VoIP Telephones
CNSSI-7003 Protected Distribution Systems (PDS)
DoDD 8521.01E Department of Defense Biometrics
DoDI 8100.04 DoD Unified Capabilities (UC)
DoDI 8523.01 Communications Security (COMSEC)
CJCSI 6510.02F Cryptographic Modernization Planning

Manage Access
HSPD-12 Policy for a Common ID Standard for Federal Employees and Contractors
NIST SP 800-210 General Access Control Guidance for Cloud Systems
CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information
CNSSP-16 National Policy for the Destruction of COMSEC Paper Material
CNSSD-507 National Directive for ICAM Capabilities...
CNSSI-1300 Instructions for NSS PKI X.509
CNSSI-4001 Controlled Cryptographic Items
CNSSI-4005 Safeguarding COMSEC Facilities and Materials, amended by CNSS-008-14
DoDI 1000.25 DoD Personnel Identity Protection (PIP) Program
DoDI 5200.08 Security of DoD Installations and Resources and the DoD PSRB
DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling
DoDM 1000.13, Vol. 1 DoD ID Cards: ID Card Life-cycle

Assure Information Sharing
CNSSP-24 Policy on Assured Info Sharing (AIS) for National Security Systems(NSS)
DoDI 8170.01 Online Information Management and Electronic Messaging
DoDI 8320.02 Sharing Data, Info, and IT Services in the DoD
CJCSI 3213.01D, Joint Operations Security

ANTICIPATE
Understand the Battlespace
FIPS 199 Standards for Security Categorization of Federal Info. and Info. Systems
NIST SP 800-60, Vol 1, R1 Guide for Mapping Types of Info and Info Systems to Security Categories
NISTIR 7693 Specification for Asset Identification 1.1
CNSSP-28 Cybersecurity of Unmanned National Security Systems

Prevent and Delay Attackers and Prevent Attackers from Staying
FIPS 200 Minimum Security Requirements for Federal Information Systems
NIST SP 800-53 R5 Security & Privacy Controls for Information Systems and Orgs.
NIST SP 800-61, R2 Computer Security Incident Handling Guide
NIST SP 800-128 Guide for Security-Focused Configuration Mgt of Info Systems
NIST SP 800-218 Secure Software Development Framework (SSDF)
CNSSI-1011 Implementing Host-Based Security Capabilities on NSS
CNSSI-1253 Security Categorization and Control Selection for Nat'l Security Systems
CNSSAM IA 1-10, Reducing Risk of Removable Media in NSS
DoDI 5200.39 CPI Identification and Protection within RDT&E
DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations
DoDI 8531.01, DoD Vulnerability Management
DoDM 5105.21V1, SCI Admin Security Manual: Info and Info Sys Security
DTM 17-007 Interim Policy and Guidance for Defense Support to Cyber Incident Response
CJCSM 6510.02 IA Vulnerability Mgt Program

ABOUT THIS CHART

- This chart organizes cybersecurity policies and guidance by Strategic Goal and Office of Primary Responsibility (see Color Key). Double-clicking* on the box directs users to the most authoritative publicly accessible source.
- Policies in *italics* indicate the document is marked for limited distribution or no authoritative public-facing hyperlink is currently available.
- The linked sites are not controlled by the developers of this chart. We regularly check the integrity of the links, but you may occasionally experience an error message due to problems at the source site or the site's decision to move the document. Please let us know if you believe the link is no longer valid.
- CNSS policies link only to the CNSS site.
- Boxes with red borders reflect recent updates.
- *Note: It is best to open this PDF directly in a browser. However, if you are unable to open the links directly from this PDF document, place your cursor over the target box and right-click to copy the link location. Open a web browser and paste the copied link into the address bar.
- For the latest version of this chart or email alerts to updates go to <https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/>

Distribution Statement A: Approved for Public Release. Distribution is unlimited.

PREPARE
Develop and Maintain Trust
CNSSP-12 National IA Policy for Space Systems Used to Support NSS
NIST 800-160, Vol.1 Rev.1, Engineering of Trustworthy Secure Systems
DoDD 3020.40 Mission Assurance

Strengthen Cyber Readiness
NIST SP 800-207 Zero Trust Architecture
NIST SP 800-30, R1 Guide for Conducting Risk Assessments
NIST SP 800-126, R3 SCAP Ver. 1.3
NIST SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government
CNSSD-505 Supply Chain Risk Management
DoDD 3700.01 DoD Command and Control (C2) Enabling Capabilities
DoDI 8140.02 Identification, Tracking, and Reporting of Cyberspace Workforce Requirements
DoDI 8560.01 COMSEC Monitoring

Sustain Missions
NIST SP 800-34, R1 Contingency Planning Guide for Federal Information Systems
CNSSP-18 National Policy on Classified Information Spillage
CNSSP-300 National Policy on Control of Compromising Emanations
CNSSI-4004.1, Destruction and Emergency Protection Procedures for COMSEC and Class. Material
CNSSI-7000 TEMPEST Countermeasures for Facilities
DoDD 3020.26 DoD Continuity Policy
DoDD 5144.02 DoD Chief Information Officer
DoDI 5000.83 Technology & Program Protection to Maintain Technological Advantage
ICD 503 IT Systems Security Risk Management and C&A
NSA IA Directorate (IAD) Management Directive MD-110 Cryptographic Key Protection

Color Key - OPRs

DOD CIO	NIST	USD(I&S)
CNSS/NSTISS	NSA	USD(P)
DISA	OSD	USD(P&R)
DNI	CYBERCOM	Other Agencies
JCS	USD(A&S)	Recently updated policy and/or link Expired, Update pending
NIAP	USD(C)	

AUTHORITIES
Title 10, US Code Armed Forces (§§2224, 3013(b), 5013(b), 8013(b))
Title 32, US Code National Guard (§102)
Title 44, US Code Federal Information Security Mod. Act. (Chapter 35)
Clinger-Cohen Act, Pub. L. 104-106
Title 14, US Code Cooperation With Other Agencies (Ch. 7)
Title 40, US Code Public Buildings, Property, and Works (Ch. 113: §§11302, 11315, 11331)
Title 50, US Code War and National Defense (§§3002, 1801)
UCP Unified Command Plan (US Constitution Art II, Title 10 & 50)

NATIONAL / FEDERAL
Computer Fraud and Abuse Act Title 18 (§1030)
Stored Communications Act Title 18 (§2701 et seq.)
Foreign Intelligence Surveillance Act Title 50 (§1801 et seq)
Executive Order 13526 Classified National Security Information
Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing
EO 13800: Strengthening Cybersecurity of Fed Nets and CI
EO 13873: Securing the Information and Communications Technology and Services Supply Chain
NSPD 54 / HSPD 23 Computer Security and Monitoring
PPD 41: United States Cyber Incident Coordination
FAR Federal Acquisition Regulation
Ethics Regulations
NIST Special Publication 800-Series
NIST SP 800-88, R1 Guidelines for Media Sanitization
NIST SP 800-125A, R1, Security Recommendations for Hypervisor Platforms
NIST SP 800-209 Security Guidelines for Storage Infrastructure
CNSSD-502 National Directive On Security of National Security Systems
CNSSD-900, Governing Procedures of the Committee on National Security Systems
DoD Information Technology Environment Strategic Plan
Federal Wiretap Act Title 18 (§2510 et seq.)
Pen Registers and Trap and Trace Devices Title 18 (§3121 et seq.)
Executive Order 13231 as Amended by EO 13286 - Critical Infrastructure Protection in the Info Age
Executive Order 13587 Structural Reforms To Improve Classified Nets
EO 13636: Improving Critical Infrastructure Cybersecurity
NSD 42, National Policy for the Security of Nat'l Security Telecom and Information Systems
EO 14028: Improving the Nation's Cybersecurity
PPD 21: Critical Infrastructure Security and Resilience
PPD 28, Signals Intelligence Activities
A-130, Management of Fed Info Resources
Joint Special Access Program (SAP) Implementation Guide (JSIG)
NIST SP 800-63 series Digital Identity Guidelines
NIST SP 800-101, R1 Guidelines on Mobile Device Forensics
NIST SP 800-137 Information Security Continuous Monitoring (ISCM)
NISTIR 7298, R3, Glossary of Key Information Security Terms
CNSSD-901 Nat'l Security Telecom's and Info Sys Security (CNSS) Issuance System
CNSSI-4009 Cmte on National Security Systems Glossary
RMF Knowledge Service

OPERATIONAL/SUBORDINATE POLICY
CYBERCOM Orders
JFHQ-DODIN Orders
DoD Security Classification Guides
Security Configuration Guides (SCGs)
Component-level Policy (Directives, Instructions, Publications, Memoranda)
Security Technical Implementation Guides (STIGs)