CSIAC Cyber Security & Information Systems Information Analysis Center

Build and Operate a Trusted DoDIN

Cybersecurity-Related Policies and Issuances
Developed by the DoD Deputy CIO for Cybersecurity
Last Updated: February 26, 2024
Send questions/suggestions to contact@csiac.org

ORGANIZE

Lead and Govern

2022 National Security Strategy	2022 National Defense Strategy (NDS)	2022 National Military Strategy (NMS)	2023 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
2022 DoD Zero Trust Strategy	2023 DoD Cyber Strategy Summary	DoD Cyber Workforce Strategy	DoD Digital Modernization Strategy	2023 DoD Data, Analytics, and Artificial Intelligence Adoption Strategy	DoD OCONUS Cloud Strategy	DoD Identity, Credential, and Access Management (ICAM) Strategy	DoD 5G Strategy	DoD Software Modernization Strategy	DoD Information Security Continuous Monitoring (ISCM) Strategy	DoD Strategy for Operations in the Information Environment

United States Intelligence Community Information Sharing Strategy

ORGANIZE

Design for the Fight

NIST SP 800-119 Guidelines for the Secure Deployment of IPv6	CNSSP-11 Nat'l Policy Governing the Acquisition of IA and IA-Enabled IT
CNSS National Secret Fabric Architecture Recommendations	DFARS Subpart 208.74, Enterprise Software Agreements
DoDD 5000.01 Defense Acquisition Framework	DoDD O-5100.19 (CAC req'd) Critical Information Communications (CRITCOM) System
DoDD 5200.47E Anti-Tamper (AT)	DoDD 7045.20 Capability Portfolio Management
DoDD 8115.01 IT Portfolio Management	DoDI 5000.02 Operation of the Adaptive Acquisition Framework
DoDI 5000.82 Requirements for the Acquisition of Digital Capabilities	DoDI 5000.87 Operation of the Software Acquisition Pathway
DoDI 8580.1 Information Assurance (IA) in the Defense Acquisition System	DoDI 7000.14 Financial Management Policy and Procedures (PPBE)
DoDI 8115.02 IT Portfolio Management Implementation	DoDI 8310.01 Information Technology Standards in the DoD
DoDI 8330.01 Interoperability of IT and National Security Systems (NSS)	DoDI 8510.01 Risk Management Framework for DoD IT
DODAF (Version 2.02) DoD Architecture Framework	MOA between DoD CIO and ODNI CIO Establishing Net-Centric Software Licensing Agreements
DoD Cybersecurity Reference Architecture (Version 5.0)	CJCSI 6510.01F Information Assurance (IA) and Computer Network Defense (CND)
CJCSI 5123.01I Charter of the JROC and Implementation of the JCIDS	

Develop the Workforce

NIST SP 800-181 R1 Workforce Framework for Cybersecurity	CNSSI-4016 National IA Training Standard For Risk Analysts
CNSSD-504 Protecting National Security Systems from Insider Threat	CNSSI-4000 Maintenance of Communications Security (COMSEC) Equipment
CNSSI-4013 National IA Training Standard For System Administrators (SA)	CNSSI-4012 National IA Training Standard for Senior Systems Managers
NSTISSI-4015 National Training Standard for System Certifiers	CNSSI-4014 National IA Training Standard For Information Systems Security Officers
DoDI 8140.02 Identification, Tracking, And Reporting of Cyberspace Workforce Requirements	DoDD 8140.01 Cyberspace Workforce Management
DoDD 5101.23E DoD Executive Agent for Advanced Cyber Training Curricula	DoDM 3305.09 Cryptologic Accreditation and Certification
DODM 8140.03 Cyberspace Workforce Qualification and Management Program	

Partner for Strength

NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing	NIST SP 800-171, R2 Protecting CUI in Nonfederal Systems and Organizations
NIST SP 800-172A Enhanced Security Requirements for Protecting CUI	CNSSP-14 National Policy Governing the Release of IA Products/Services…
CNSSI-4008 Program for the Mgt and Use of Nat'l Reserve IA Security Equipment	DoDI 5205.13 Defense Industrial Base (DIB) Cyber Security (CS) / IA Activities
DoDM O-5205.13 *DIB CS/IA Program Security Classification Manual*	DoD 5220.22-M, Ch. 2 National Industrial Security Program Operating Manual (NISPOM)
Cybersecurity Maturity Model Certification (CMMC)	MOA Between DoD and DHS (Jan. 19, 2017)

ENABLE

Secure Data in Transit

FIPS 140-3 Security Requirements for Cryptographic Modules	NIST SP 800-153 Guidelines for Securing Wireless Local Area Networks
NIST SP 1800-22 Mobile Device Security: Bring Your Own Device (BYOD)	CNSSP-1 National Policy for Safeguarding and Control of COMSEC Material
CNSSP-15 Use of Pub Standards for Secure Sharing of Info Among NSS	CNSSP-17 Policy on Wireless Communications: Protecting Nat'l Security Info
CNSSP-19 National Policy Governing the Use of HAIPE Products	CNSSP-25 National Policy for PKI in National Security Systems
NSTISSP-101 National Policy on Securing Voice Communications	*NACSI-2005* *Communications Security (COMSEC) End Item Modification*
CNSSI-5000 Voice Over Internet Protocol (VoIP) Computer Telephony (Annex I, VoSIP)	CNSSI-5001 Type-Acceptance Program for VoIP Telephones
NACSI-6002 Nat'l COMSEC Instruction Protection of Gov't Contractor Telecomm's	CNSSI-7003 Protected Distribution Systems (PDS)
DoDD 8100.02 Use of Commercial Wireless Devices, Services, and Tech in the DoD GIG	DoDD 8521.01E Department of Defense Biometrics
DoDI 4650.01 Policy and Procedures for Mgt and Use of the Electromagnetic Spectrum	DoDI 8100.04 DoD Unified Capabilities (UC)
DoDI 8420.01 Commercial WLAN Devices, Systems, and Technologies	DoDI 8523.01 Communications Security (COMSEC)
DoDI S-5200.16 *Objectives and Min Stds for COMSEC Measures used in NC2 Comms*	CJCSI 6510.02F Cryptographic Modernization Planning

Manage Access

HSPD-12 Policy for a Common ID Standard for Federal Employees and Contractors	FIPS 201-3 Personal Identity Verification (PIV) of Federal Employees and Contractors
NIST SP 800-210 General Access Control Guidance for Cloud Systems	NIST SP 1800-16 Securing Web Transactions: TLS Server Certificate Management
CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information	CNSSP-10 Nat'l Policy Gov. Use of Approved Sec. Containers in Info Security Applications
CNSSP-16 National Policy for the Destruction of COMSEC Paper Material	CNSSP-200 National Policy on Controlled Access Protection
CNSSD-507 National Directive for ICAM Capabilities...	CNSSD-506 National Directive to Implement PKI on Secret Networks
CNSSI-1300 Instructions for NSS PKI X.509	NSTISSI-3028 Operational Security Doctrine for the FORTEZZA User PCMCIA Card
CNSSI-4001 Controlled Cryptographic Items	CNSSI-4003 Reporting and Evaluating COMSEC Incidents
CNSSI-4005 Safeguarding COMSEC Facilities and Materials, amended by CNSS-008-14	CNSSI-4006 Controlling Authorities for COMSEC Material
DoDI 1000.25 DoD Personnel Identity Protection (PIP) Program	DoDI 5200.01 DoD Information Security Program and Protection of SCI
DoDI 5200.08 Security of DoD Installations and Resources and the DoD PSRB	DoDI 5200.48 Controlled Unclassified Information(CUI)
DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling	DoDI 8520.03 Identity Authentication for Information Systems
DoDM 1000.13, Vol. 1 DoD ID Cards: ID Card Life-cycle	DoDM 5205.02 DoD Operations Security (OPSEC) Program Manual

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	DoDI 8582.01 Security of Non-DoD Info Sys Processing Unclassified Nonpublic DoD Information
CJCSI 3213.01D, Joint Operations Security	CJCSI 6211.02D Defense Information System Network: (DISN) Responsibilities

ANTICIPATE

Understand the Battlespace

FIPS 199 Standards for Security Categorization of Federal Info. and Info. Systems	NIST SP 800-59 Guideline for Identifying an Information System as a NSS
NIST SP 800-60, Vol 1, R1 Guide for Mapping Types of Info and Info Systems to Security Categories	NIST SP 800-92 Guide to Computer Security Log Management
NISTIR 7693 Specification for Asset Identification 1.1	CNSSP-28 Cybersecurity of Unmanned National Security Systems
NSTISSD-600 Communications Security Monitoring	*DoDI S-5240.23* *Counterintelligence (CI) Activities in Cyberspace*

Prevent and Delay Attackers and Prevent Attackers from Staying

FIPS 200 Minimum Security Requirements for Federal Information Systems	NIST SP 800-37 R2 Guide for Applying the Risk Mgt Framework to Fed. Info. Systems
NIST SP 800-53 R5 Security & Privacy Controls for Information Systems and Orgs.	NIST SP 800-53A R5 Assessing Security & Privacy Controls in Information Systems & Orgs.
NIST SP 800-61, R2 Computer Security Incident Handling Guide	NIST SP 800-124, R2 Guidelines for Managing the Security of Mobile Devices in the Enterprise
NIST SP 800-128 Guide for Security-Focused Configuration Mgt of Info Systems	NIST SP 800-163, R1 Vetting the Security of Mobile Applications
NIST SP 800-218 Secure Software Development Framework (SSDF)	NIST SP 1800-26 Data Integrity: Detecting & Responding to Ransomware
CNSSI-1011 Implementing Host-Based Security Capabilities on NSS	CNSSI-1013 Network Intrusion Detection Sys & Intrusion Prevention Sys (IDS/IPS)
CNSSI-1253 Security Categorization and Control Selection for Nat'l Security Systems	CNSSI-1253F, Atchs 1-5 Security Overlays
CNSSAM IA 1-10, Reducing Risk of Removable Media in NSS	DoDI 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers
DoDI 5200.39 CPI Identification and Protection within RDT&E	DoDI 5205.83 DoD Insider Threat and Management and Analysis Center
DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations	DoDI 8530.03 Cyber Incident Response
DoDI 8531.01, DoD Vulnerability Management	DoDI 8551.01 Ports, Protocols, and Services Management (PPSM)
DoDM 5105.21V1, SCI Admin Security Manual: Info and Info Sys Security	DoDM 8530.01 Cybersecurity Activities Support Procedures
DTM 17-007 Interim Policy and Guidance for Defense Support to Cyber Incident Response	CJCSM 6510.01B Cyber Incident Handling Program
CJCSM 6510.02 *IA Vulnerability Mgt Program*	Joint Publication 6-0 Joint Communications System

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	CNSSP-21 National IA Policy on Enterprise Architectures for NSS
NIST 800-160, Vol.1 Rev.1, Engineering of Trustworthy Secure Systems	CNSSI-5002, Telephony Isolation Used for Unified Comms. Implementations w/ in Physically Protected Spaces
DoDD 3020.40 Mission Assurance	DoDD 3100.10 Space Policy

Strengthen Cyber Readiness

NIST SP 800-207 Zero Trust Architecture	NIST SP 800-18, R1 Guide for Developing Security Plans for Federal Information Systems
NIST SP 800-30, R1 Guide for Conducting Risk Assessments	NIST SP 800-39 Managing Information Security Risk
NIST SP 800-126, R3 SCAP Ver. 1.3	NIST SP 1800-25 Data Integrity: Identifying and Protecting Assets Against Ransomware
NIST SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government	NIST SP 800-221 Enterprise Impact of Information and Communications Technology Risk
CNSSP-32 Cloud Security for National Security Systems	CNSSD-505 Supply Chain Risk Management
CNSSD-520 The Use of Mobile Devices to Process Nat'l Sec. Info. Outside Secure Spaces	DoDD 3700.01 DoD Command and Control (C2) Enabling Capabilities
DoDD 5101.21E Unified Platform and Joint Cyber Command and Control (JCC2)	DoDI 8560.01 COMSEC Monitoring
DoDI 8500.01 Cybersecurity	DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems / Networks

Sustain Missions

NIST SP 800-34, R1 Contingency Planning Guide for Federal Information Systems	NIST SP 800-82, R3 Guide to Operational Technology (OT) Security
CNSSP-18 *National Policy on Classified Information Spillage*	CNSSP-22, IA Risk Management Policy for National Security Systems
CNSSP-300 *National Policy on Control of Compromising Emanations*	*CNSSI-1001* *National Instruction on Classified Information Spillage*
CNSSI-4004.1, Destruction and Emergency Protection Procedures for COMSEC and Class. Material	CNSSI-4007 Communications Security (COMSEC) Utility Program
CNSSI-7000 *TEMPEST Countermeasures for Facilities*	*NSTISSI-7001* *NONSTOP Countermeasures*
DoDD 3020.26 DoD Continuity Policy	DoDD 3020.44 Defense Crisis Management
DoDD 5144.02 DoD Chief Information Officer	DoDD 8000.01 Management of the DOD Information Enterprise
DoDI 5000.83 Technology & Program Protection to Maintain Technological Advantage	DoDI 8410.02 Support to DoD Information Network Operations
ICD 503 IT Systems Security Risk Management and C&A	UFC 4-010-06, Cybersecurity of Facility-Related Control Systems
NSA IA Directorate (IAD) Management Directive MD-110 *Cryptographic Key Protection*	Defense Acquisition Guidebook Program 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
■	NIAP	■	USD(C)	□	Expired, Update pending

AUTHORITIES

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

NATIONAL / FEDERAL

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