CSIAC
266 Genese Street
Utica, NY 13502
Phone: 1-800-214-7921

Cyber Security & Information Systems Information Analysis Center

Build and Operate a Trusted DoDIN

ORGANIZE

Lead and Govern

- EO 13873: Securing the Information and Communications Technology and Services Supply Chain
- EO 13800: Strengthening Cybersecurity of Fed Nets and CI
- EO 13636: Improving Critical Infrastructure Cybersecurity
- PPD 41: United States Cyber Incident Coordination
- PPD 21: Critical Infrastructure Security and Resilience
- National Cyber Strategy
- U.S. Int'l Strategy for Cyberspace
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- 2017 National Security Strategy
- CNSSP-24 Policy on Assured Info Sharing (AIS) for National Security Systems(NSS)
- National Defense Strategy (NDS)
- 2019 National Intelligence Strategy
- National Military Strategy (NMS)
- DoD Cloud Strategy
- 2018 DoD Cyber Strategy
- DoD Digital Modernization Strategy
- DoDD 8000.01 Management of the DOD Information Enterprise
- DoDI 8500.01 Cybersecurity

Cybersecurity-Related Policies and Issuances

Developed by the DoD Deputy CIO for Cybersecurity

Last Updated: April 1, 2020

Send questions/suggestions to **info@csiac.org**

ORGANIZE

Design for the Fight

- NIST SP 800-119 Guidelines for the Secure Deployment of IPv6
- Common Criteria Evaluation and Validation Scheme (CCEVS)
- CNSSP-11 Nat'l Policy Governing the Acquisition of IA and IA-Enabled IT
- DFARS Subpart 208.74, Enterprise Software Agreements
- DoDD 5000.01 The Defense Acquisition System
- DoDD 7045.20 Capability Portfolio Management
- DoDD 8115.01 IT Portfolio Management
- DoDI 5000.02T Operation of the Defense Acquisition System
- DoDI 5200.44 Protection of Mission Critical Functions to Achieve TSN
- 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
- DoDI 8580.1 Information Assurance (IA) in the Defense Acquisition System
- RMF Knowledge Service
- MOA between DoD CIO and ODNI CIO Establishing Net-Centric Software Licensing Agreements
- DODAF (Version 2.02) DoD Architecture Framework
- CJCSI 5123.01H Charter of the JROC and Implementation of the JCID
- Joint Publication 6-0 Joint Communications System
- CNSS National Secret Fabric Architecture Recommendations
- MOA Between DoD and DHS (Jan. 19, 2017, requires CAC)

Develop the Workforce

- CNSSD-500 Information Assurance (IA) Education, Training, and Awareness
- NSTISSD-501 National Training Program for INFOSEC Professionals
- CNSSI-4000 Maintenance of Communications Security (COMSEC) Equipment
- NSTISSI-4011 National Training Standard for INFOSEC Professionals
- CNSSI-4012 National IA Training Standard for Senior Systems Managers
- CNSSI-4013 National IA Training Standard For System Administrators (SA)
- CNSSI-4014 National IA Training Standard For Information Systems Security Officers
- NSTISSI-4015 National Training Standard for System Certifiers
- CNSSI-4016 National IA Training Standard For Risk Analysts
- DoDD 8140.01 Cyberspace Workforce Management
- DoDI 8170.01 Online Information Management and Electronic Messaging
- DoD 8570.01-M Information Assurance Workforce Improvement 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
- CNSSP-14 National Policy Governing the Release of IA Products/Services…
- CNSSI-1253 Security Categorization and Control Selection for Nat'l Security Systems
- CNSSI-1253F, Atchs 1-5 Security Overlays
- CNSSI-4007 Communications Security (COMSEC) Utility Program
- 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)

ENABLE

Secure Data in Transit

- FIPS 140-3 Security Requirements for Cryptographic Modules
- NIST SP 800-153 Guidelines for Securing Wireless Local Area Networks
- 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 6510.02E Cryptographic Modernization Plan*
- *CJCSI 6510.06C Communications Security Releases to Foreign Nations*

Manage Access

- HSPD-12 Policy for a Common ID Standard for Federal Employees and Contractors
- FIPS 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors
- CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information
- CNSSP-16 National Policy for the Destruction of COMSEC Paper Material
- 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

Assure Information Sharing

- 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
- DoD Information Sharing Strategy
- United States Intelligence Community Information Sharing Strategy
- CJCSI 6211.02D Defense Information System Network: (DISN) Responsibilities
- CJCSI 3213.02D, Joint Operations Security

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
- CNSSD-520 Use of Mobile Devices to Process Nat'l Sec.Info Outside Secure Spaces
- CNSSP-28 Cybersecurity of Unmanned National Security Systems
- 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 R1 Guide for Applying the Risk Mgt Framework to Fed. Info. Systems
- NIST SP 800-53 R4 Security & Privacy Controls for Federal Information Systems
- NIST SP 800-53A R4 Assessing Security & Privacy Controls in Fed. Info. Systems & Orgs.
- NIST SP 800-61, R2 Computer Security Incident Handling Guide
- NIST SP 800-124, R1 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 Vetting the Security of Mobile Applications
- CNSSAM IA 1-10, Reducing Risk of Removable Media in NSS
- DoDI 5200.39 CPI Identification and Protection within RDT&E
- DoDI 8551.01 Ports, Protocols, and Services Management (PPSM)
- DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations
- DoD O-8530.1-M (CAC req'd) CND Service Provider Certification and Accreditation Program
- DoDM 5105.21V1, SCI Admin Security Manual: Info and Info Sys Security
- CJCSI 6510.01F Information Assurance (IA) and Computer Network Defense (CND)
- CJCSM 6510.01B Cyber Incident Handling Program
- *CJCSM 6510.02 IA Vulnerability Mgt Program*
- DTM 17-007, Ch. 2, Defense Support to Cyber Incident Response

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, Systems Security Engineering: ... 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
- DoDI 8581.01 IA Policy for Space Systems Used by the DoD
- DoDD 5144.02 DoD Chief Information Officer

Strengthen Cyber Readiness

- 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 800-126, R3 SCAP Ver. 1.3
- NIST SP 800-137 Continuous Monitoring
- NIST SP 800-39 Managing Information Security Risk
- DoDD 3700.01 DoD Command and Control (C2) Enabling Capabilities
- *DoDD S-3710.01 National Leadership Command Capability*
- DoDI 8560.01 COMSEC Monitoring
- Joint Special Access Program (SAP) Implementation Guide (JSIG)

Sustain Missions

- NIST SP 800-34, R1 Contingency Planning Guide for Federal Information Systems
- NIST SP 800-82, R2 Guide to Industrial Control Systems (ICS) 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-7000 TEMPEST Countermeasures for Facilities*
- *NSTISSI-7001 NONSTOP Countermeasures*
- DoDD 3020.26 DoD Continuity Policy
- DoDD 3020.44 Defense Crisis Management
- DoDI 8410.02 NetOps for the Global Information Grid (GIG)
- Defense Acquisition Guidebook Program Protection
- UFC 4-010-06, Cybersecurity of Facility-Related Control Systems
- ICD 503 IT Systems Security Risk Management and C&A
- *NSA IA Directorate (IAD) Management Directive MD-110 Cryptographic Key Protection*

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
- Executive Order 13526 Classified National Security Information
- Executive Order 13587 Structural Reforms To Improve Classified Nets
- Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing
- NSD 42, National Policy for the Security of Nat'l Security Telecom and Information Systems
- PPD 28, Signals Intelligence Activities
- *NSPD 54 / HSPD 23 Computer Security and Monitoring*
- A-130, Management of Fed Info Resources
- FAR Federal Acquisition Regulation
- Ethics Regulations
- National Strategy to Secure Cyberspace
- Summary of the 2018 DoD Artificial Intelligence Strategy
- NIST Special Publication 800-Series
- NIST SP 800-63 series Digital Identity Guidelines
- NIST SP 800-101, R1 Guidelines on Mobile Device Forensics
- NIST SP 800-88, R1,Guidelines for Media Sanitization
- NIST SP 800-125A, R1, Security Recommendations for Hypervisor Platforms
- NISTIR 7298, R3, Glossary of Key Information Security Terms
- CNSSD-502 National Directive On Security of National Security Systems
- CNSSD-900, Governing Procedures of the Committee on National Security Systems
- CNSSD-901 Nat'l Security Telecomm's and Info Sys Security (CNSS) Issuance System
- CNSSI-4009 Cmte on National Security Systems Glossary
- DoD Information Technology Environment Strategic Plan

OPERATIONAL

- *CYBERCOM Orders*
- *JFHQ-DODIN Orders*

SUBORDINATE POLICY

- Security Configuration Guides (SCGs)
- *Component-level Policy (Directives, Instructions, Publications, Memoranda)*
- NSA IA Guidance
- Security Technical Implementation Guides (STIGs)

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 check the integrity of the links on a regular basis, 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, per restrictions implemented by its website design.
- Boxes with red borders reflect recent updates.
- Note: Users of the iPad, iPhone or iPod Touch may find they can view this Chart but that its hyperlinks are inoperable, because of Apple's decision not to fully support certain Adobe products. For those who desire a workaround for this issue, there are apps in the iTunes store for less than $1.00.
- For the latest version of this chart go to https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/. You can sign up to be alerted by e-mail to any updates to this document.

Color Key - OPRs

- ASD(NII)/ASD(C3I) /DOD CIO
- CNSS/NSTISS
- DISA
- DNI
- JCS
- NIAP
- NIST
- NSA
- OSD
- CYBERCOM
- USD(A&S)
- USD(C)
- USD(I)
- USD(P)
- USD(P&R)
- Other Agencies
- Recently updated policy and/or link
- Expired, Update pending

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