

Cybersecurity and Cyberspace Operations

LCDR Steve Albert, USCG Office of Cyberspace Forces (CG-791)

Sea Air Space 2021

Cybersecurity and Cyberspace Operations



What is Cyberspace?



UNITED STATES COAST GU. * * * * * CYBER STRATE

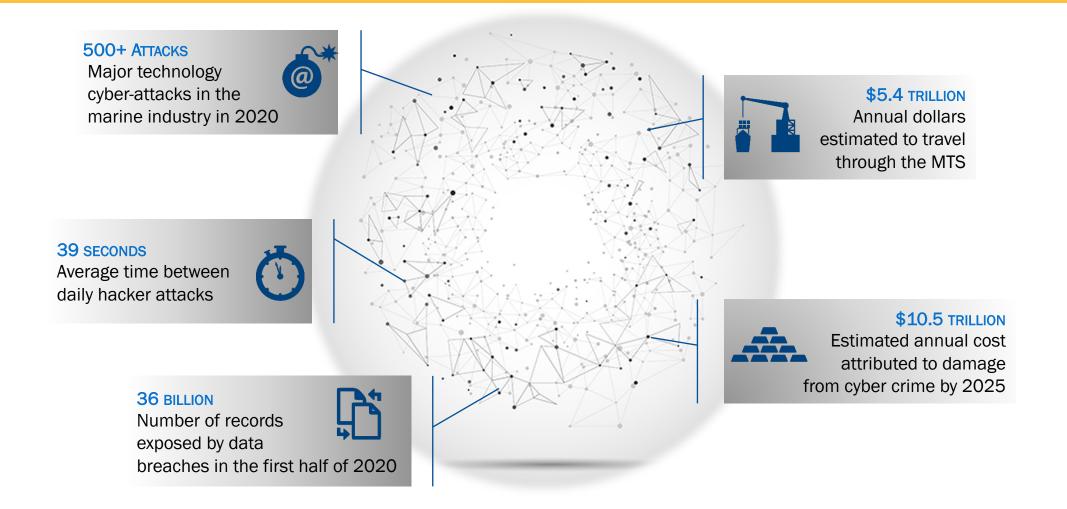
> JUNE 2015 WASHINGTON, D.C.

Exciting News!



Office of Cyberspace Forces (CG-791)

Why is Cyberspace Important?



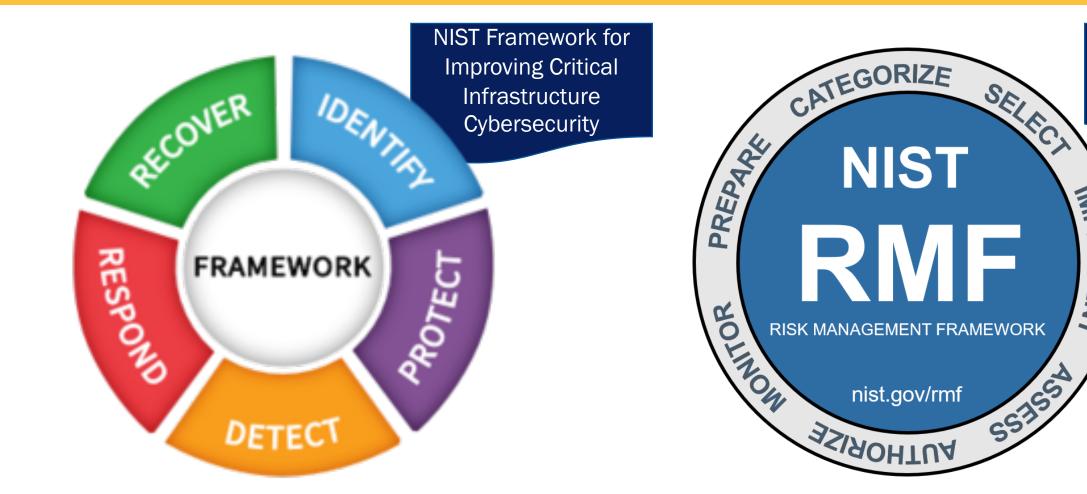


U.S. Coast Guard Cybersecurity and Cyberspace Operations





Securing U.S. Coast Guard Cyberspace





NIST SP

800-53

MPLEMENT

Future of U.S. Coast Guard Cyberspace Operations

Defend and Operate the Enterprise Mission Platform

The U.S. Coast Guard must defend and operate the U.S. Coast Guard Enterprise Mission Platform (EMP), our portion of the Department of Defense (DOD) Information Network (DODIN), including all U.S. Coast Guard technology.

Protect the Marine Transportation System (MTS)

The U.S. Coast Guard will employ frameworks, standards, and best practices in prevention and response activities to identify and manage cyber risks to the MTS.

Operate in and through Cyberspace

The U.S. Coast Guard will embed cyber planning in our traditional missions and plan to execute cyberspace operations that combine the Service's unique authorities, capabilities, and workforce to deliver mission success.

Improving Acquisition Cybersecurity



Valuable U.S. Coast Guard Cyber Targets



Securing the Supply Chain





Security Policy & Technology Familiarization

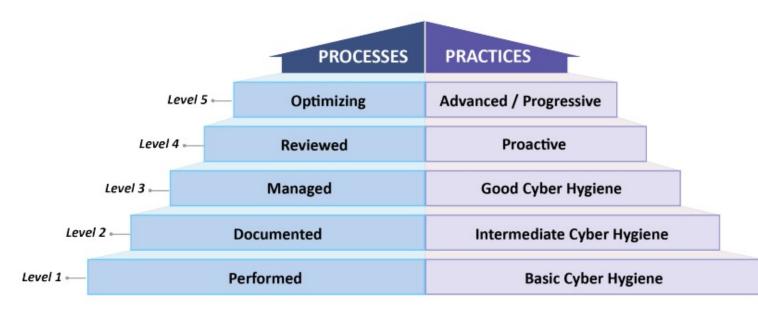
Cybersecurity-Related Developed by the DoD										
ORGANIZE Deputy CIO for Cybersecurity										
Lead and Govern Lead and Govern Send Gover										
niejm Netional Recutly Bratagic Galdance	United States Intelligence Community Information Sharing Strategy		.5. Intil Statiogy for Cyberspace				nat Defense Bindagy (HDS)	iaitonal Millary Statingy (1647)	info@csiac.org	
2018 DeD Cytwr Stralegy	DeD Digital Modernization Breakgy	DaD Cybernerardy Rait Rankuslan Sinningy	Summary of the 2018 DoD Artificial Intelligence Strategy	DuD Cloud Boology	DoD Dels Strategy	islantily, Consiential, anal Access lanagement (CAAA) Heatingy	DeD 80 Statingy Do	oD Information Sharing Strategy		
ORG	ANIZE	ENABLE		ANTICIPATE		РІ	PREPARE		AUTHORITIES Tite 19, US Code Tite 14, US Code	
Design for the Fight		Secure Data in Transit		Understand the Battlespace		Develop ar	Develop and Maintain Trust		Title 14, US Code Cooperation With Other Agencies (Ch. 7)	
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	FIPS 140-3 Security Requirements for Cryptographic Modules	NIST SP 800-153 Guidelines for Securing Wireless Local Area Networks	FIPS 199 Standards for Security Categorizal of Federal Into. and Into. System		CNSSP-12 National IA Policy for Space System Used to Support NSS	Architectures for NSS		(cit. r) Title 40, US Code Public Buldings, Property, and Works (Cit. 113: 5511302, 11315, 11331)	
CNSS National Secret Fabric Architecture Recommendiations	DFARS Subpart 208.74, Enterprise Software Agreements	CNSSP-1 National Policy for Safeguarding and Control of COMSEC Material CNSSP-17	CNSSP-15 Use of Pub Standards for Secure Sharing of Into Among NSS CNSSP-19	NIST SP 800-60, Vol 1, R1 Guide for Mapping Types of into a into Systems to Security Categori		NIST 800-160, vol. 1, Systems Securi Engineering: Engineering of Trustworthy Secure Systems	ty CNSSI-5002, Telephony isolation for Unified Comms. Implementatio In Physically Protected Space	Used ns w/ ss Federal information Security Mod. Act, (Chapter 35)	Title 50, US Code War and National Detense (§§3002, 1801)	
DoDD 5000.01 The Defense Acquisition System	DoDD O-\$100.19 (CAC reg'd) Critical Information Communications (CRITCOM) System	Policy on Wireless Communications: Protecting Nat'l Security Info	National Policy Governing the Use of HAIPE Products	NISTIR 7693 Specification for Asset Identification	CNSSD-520 Use of Mobile Devices to Process Na Sec. Info Outside Secure Spaces	t1 DoDD 3020.40 Mission Assurance	DoDD 3100.10 Space Policy	Clinger-Cohen Act, Pub. L. 104-106	UCP United Command Plan (US Constitution Art II, Title 10 & 50)	
DoDD 7045.20 Capability Portfolio Management	DoDD 8115.01 IT Portfolio Management	CNSSP-25 National Policy for PKI in National Security Systems	NSTISSP-101 National Policy on Securing Volce Communications	CNSSP-28 Cybersecurity of Urmanned Natio Security Systems	DoDI S-5240.23 Counterintelligence (CI) Activities in Cyberspace	Strengthen	Cyber Readiness	NATIONAL	/FEDERAL	
DcDI 5000.02T Operation of the Defense Acquisition System	DoDI 5000.87 Operation of the Software Acquisition Pathway	NACSI-2005 Communications Security (COMSEC) End Item Modification	CNSSI-5000 Voice Over Internet Protocol (VoIP) Computer Telephony (Annex I, VoSIP) NACSI-6002	Prevent a	nd Delay Attackers Attackers from Staving	NIST SP 800-18, R1 Guide for Developing Security Plant for Federal Information Systems	NIST SP 800-30, R1 Guide for Conducting Risk Assessments	Computer Fraud and Abuse Act Tibe 18 (§1030)	Federal Wiretap Act Title 18 (§2510 et seq.)	
DoDI 5200.44 Protection of Mission Critical Functions to Achieve TSN	DoDI 7000.14 Financial Management Policy and Procedures (PPBE)	CNSSI-5001 Type-Acceptance Program for VoIP Telephones	Natl COMSEC instruction Protection of Gov1 Contractor Telecomm's	FIPS 200 Minimum Security Requirements t Federal Information Systems	NIST SP 800-37 R2 Guide for Applying the Risk Mgt Framework to Fed. Info. Systems	NIST SP 800-126, R3 SCAP Ver. 1.3	NIST SP 800-137 Continuous Monitoring	Stored Communications Act Title 18 (§2701 et seq.)	Pen Registers and Trap and Trace Devices Title 18 (§3121 et seq.)	
DoDI 8115.02 IT Portbilo Management Implementation	DoDI 8310.01 Information Technology Standards In the DoD	CNSSI-7003 Protected Distribution Systems (PDS)	Use of Commercial Wireless Devices, Services, and Tech in the DoD GIG	NIST SP 800-53 R5 Security & Privacy Controls for Federal Information Systems	NIST SP 800-53A R4 Assessing Security & Privacy Control In Fed. Info. Systems & Orgs.	NIST SP 800-39 Managing information Security Risk	NIST SP 1800-25 Data Integrity Identifying and Protecting Asset Against Ransomware	Foreign Intelligence Surveillance Act Title 50 (§1801 et seq)	Executive Order 13231 as Amended by EO 13286 - Ortical Infrastructure Protection in the Info Age	
DoDI 8330.01 Interoperability of IT and National Security Systems (NSS)	DoDI 8510.01 Risk Management Framework för DoD IT	DoDD 8521.01E Department of Defense Biometrics DoDI 8100.04 DoDI 8100.04	Policy and Procedures for Mgt and Use of the Electromagnetic Spectrum DoOI 8420.01 Commercial WLAN Devices, Systems, and Technologies	NIST SP 800-61, R2 Computer Security Incident Handli Guide	NIST SP 800-124, R1 Guidelines for Managing the Security o Mobile Devices in the Enterprise	DoOD 3700.01 DoD Command and Control (C2) Enabling Capabilities			Executive Order 13587 Structural Reforms To Improve Classified Nets	
DoDI 8580.1 Information Assurance (IA) in the Defense Acquisition System	RMF Knowledge Service	DoDI 8523.01 Communications Security (COMSEC)	DoDI S-5200.16 Objectives and Min Stds for COMSEC	NIST SP 800-128 Guide for Security-Focused Configuration Mgt of Info Systems	NIST SP 800-163, R1 Vetting the Security of Mobile Applications	DoDD 5101.21E United Platform and Joint Cyber Command and Control (JCC2	DoDI 8500.01 Cybersecurity	Executive Order 13691 Promoting Pitvate Sector Cybersecurity Information Sharing	EO 13636: Improving Critical Infrastructure Cybersecurity	
MOA between DoD CIO and ODNI CIO Establishing Net-Centric Software Licensing Agreements	DODAF (Version 2.02) DoD Architecture Framework	CJCSI 0510.02E Cryptographic Modemization Plan	Measures used in NC2 Comms CJCSI 8510.08C Communications Security Releases to Foreign Nations	NIST SP 1800-26 Data Integrity: Detecting & Respond to Ransomware			Joint Special Access Program (S/ Implementation Guide (JSIG)		NSD 42, National Policy for the Security of Nat1 Security Telecom and Information Systems	
DTM 20-004 Enabling Cyberspace Accountability of DoD Components and Information Systems	Common Criteria Evaluation and Validation Scheme (CCEVS)	Manage	e Access	CNSSI-1253F, Alchs 1-5 Security Overlays	CNSSAM IA 1-10, Reducing Risk of Removable Media in NSS	Sust	in Missions	EO 13873: Securing the Information and Communications Technology and Services Supply Chain	Executive Order on Improving the Nation's Cybersecurity	
CJCSI 5123.01H Charter of the JROC and Implementation of the JCID	Joint Publication 6-0 Joint Communications System	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	DoDI 5000.90, Cybersecurity for Acquisition Decision Authorities an Program Managers	RDT&E	Enderal Information Surfame	NIST SP 800-82, R2 Guide to Industrial Control Syste (ICS) Security	NSPD 54 / HSPD 23 Computer Security and Monitoring	PPD 21: Critical Infrastructure Security and Resilience	
Develop th	e Workforce	NIST SP 800-207 Zero Trust Architecture	NIST SP 800-210 General Access Control Guidance for Cloud Systems	DoDI 5205.83 DoD Insider Threat and Manageme and Analysis Center		CNSSP-18 National Policy on Classified Information Spillage	CNSSP-22, IA Risk Manageme Policy for National Security Syst	DDD 44: United States School builded	PPD 28, Signais Intelligence Activities	
NIST SP 800-181 R1 Workforce Framework for Cybersecurity	CNSSD-500 Information Assurance (IA) Education, Training, and Awareness	NIST SP 1800-16 Securing Web Transactions: TLS Server Certificate Management	CNSSP-16 National Policy for the Destruction of COMSEC Paper Material	DoDI 8531.01, DoD Vulnerability Management	Management (PPOM)	CNSSP-300 National Policy on Control of Compromising Emanations	CNSSI-1001 National Instruction on Classifi Information Spillage	FAR Federal Acquisition Regulation	A-130, Management of Fed Info Resources	
NSTISSD-501 National Training Program for INFOSEC Professionals	CNSSI-4000 Maintenance of Communications Security (COMSEC) Equipment	CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information CNSSD-506	CNSSD-507 National Directive for ICAM Capabilities	DoD O-8530.1-M (CAC regid) CND Service Provider Certification : Accreditation Program	CJCSI 6510.01F	CNSSI-4004.1, Destruction and Emergency Protection Procedures t COMSEC and Class. Material	CNSSI-4007 Communications Security (COM: Utility Program	SEC) National Strategy to Secure Cyberspace	Ethics Regulations	
NSTISSI-4011 National Training Standard for INFOSEC Professionals	CNSSI-4012 National IA Training Standard for Senior Systems Managers CNSSI-4014	National Directive to implement PKI on Secret Networks	CNSSI-1300 Instructions for NSS PKI X.509 CNSSI-4001	to Cyber Incident Response	Computer Network Defense (CND)	CNSSI-7000 TEMPEST Countermeasures for Facilities	NSTISSI-7001 NONSTOP Countermeasure	NIST Special Publication 800-Series	NIST SP 800-63 series Digital identity Guidelines	
CNSSI-4013 National IA Training Standard For System Administrators (SA) NSTISSI-4015	National IA Training Standard For Information Systems Security Officers	Operational Security Doctrine for the FORTEZZA User PCMCIA Card CNSSI-4003 Reporting and Evaluation COMSEC	Controlled Cryptographic Items	Cyber Incident Handling Program	n IA Vulnerability Mgt Program	DeDD 3020.26 DeD Continuity Policy	DoDD 3020.44 Defense Cifsis Management	MIGT OD BOD JOEA, DJ. Demeter	NIST SP 800-101, R1 Guidelines on Mobile Device Forensios NIST SP 800-209	
NSTISSI-4015 National Training Standard for System Certifiers	National IA Training Standard For Risk Analysis	Reporting and Evaluating COMSEC Incidents CNSSI-4006 Controlling Authorities for COMSEC Material	Sateguarding COMSEC Facilities and Materials, amended by CNSS-008-14 DoD Personnel identity Protection (PIP) Program	 This chart organizes cyberse 	JT THIS CHART ecurity policies and guidance by Strateg	DoDD 5144.02 DoD Chief Information Officer	DoDD 8000.01 Management of the DOD Informa Enterprise DoDI 6410.02	ation Platforms	NIST SP 800-209 Security Guidelines for Storage Infrastructure CNSSD-502	
DoDD 8140.01 Cyberspace Workforce Management DoDM 3305.09	Online Information Management and Electronic Messaging DoD 8570.01-M Information Assurance Workforce Improvement Program	Material DoDI 5200.01 DoD Information Security Program and Protection of SCI	(PIP) Program DoDI 5200.08 Security of DoD Installations and Resources and the DoD PSRB	clicking* on the box directs u accessible source.	Responsibility (see Color Key). Double- users to the most authoritative publicly e document is marked for limited	DoDI 5000.83 Technology & Program Protection to Maintain Technological Advantage	O NetOps for the Global Informati Grid (GIG)	Outpool and America Department	CNSSD-502 National Directive On Security of National Security Systems CNSSD-901 Nati Security Telecomms and Into Sys Security (CNSS) issuance System	
Cryptologic Accreditation and Certification		DoDI 5200.48 Controlled Unclassified Information(CUI)	Public Key (PK) Enabling	distribution or no authoritativ available.	e document is marked for limited re public-facing hyperlink is currently trolled by the developers of this chart. W	ICD 503 IT Systems Security Risk Manageme and C&A	UFC 4-010-06, Cybersecurity of Pacity-Relat Control Systems	CNSSL4009	DoD Information Technology Environment Strategic Plan	
Partner 6 NIST SP 800-144 Guidelines on Security and Phyacy In Public Cloud Computing	NIST SP 800-171, R2 Protecting CUI In Nonfederal Systems and Organizations	DoDI 8520.03 Identity Authentication for Information Systems	DoDM 1000.13, Vol. 1 DoD ID Cards: ID Card Life-cycle	regularly check the integrity experience an error message	of the links, but you may occasionally e due to problems at the source site or th focument. Please let us know if you	Directive MD-110 Cryptographic Key Protection	nt Defense Acquisition Guideboo Program Protection		Environment Strategic Plain	
	NIST SP 800-172 CNSSP-14		DoDM 5205.02 DoD Operations Security (OPSEC) Program Manual		believe the link is no longer valid. CNSS policies link only to the CNSS site. Boxes with red borders reflect recent updates		NET USO(4.5)	CYBERCOM Orders	JFHQ-DODIN Orders	
Protecting CUI CNSSI-4008 Program for the Mgt and Use of Nat'l	Protecting CUI of IA Products/Sterilices CNSSI-4005 Program for the Mg1 and Use of Nat'l Reserve IA Security Equipment Defense Industrial Base (DB) Cyber Security (CS) / IA Addition		Assure Information Sharing CNSSP-24 DxDI 8320.02		 "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-dick to copy the link location. 		NSA (190(P) OND (190(P)R)	SUBORDIN	ATE POLICY	
Reserve IA Security Equipment DoDM O-5205.13 DIB CSNA Program Security Classification Manual	Security (CS) / IA Additities DoD 5220.22-M, Ch. 2 National Industrial Security Program Operating Manual (NISPOM)	CNSSP-24 Policy on Assured into Sharing (AIS) for National Security Systems(NSS) DoDI 8582.01 Security of Non-DoD Into 8ys Processing	Sharing Data, Info. and IT Services in the DoD CJCSI 3213.01D, Joint Operations Security		iste the copied link into the address bar. chart or email alerts to updates go to (bersecurity-policy-chart/	". DBA DBA DN	CYBERCON Cher Agende	(SCGs)	Component-level Policy (Directives, Instructions, Publications, Memorande)	
Cybersecurity Maturity Model Certification (CMMC)	MOA Between DoD and DHS (Jan. 19, 2017)	Unclassified Nonpublic DoD Information Unclassified Nonpublic DoD Information CJCSI 6211.02D Defense Information System Network (DISN) Responsibilities		Distribution Statement Distribution is unlimited	A: Approved for Public Release d.		UBD(C) Deter and/or 1 UBD(C) Depley and/or 1 Update pendi	Ink	Security Technical Implementation Guides (STIGs)	

DoD Cybersecurity Policy Chart

- Zero Trust
- DODAF
- Public Key
 Infrastructure
- Ransomware
- Risk Management
- Ports, Protocols, and Services Management

Improve Your Organization's Cyberspace Operations









Cyber Supply Chain Risk Management (C-SCRM)



Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities.

IDENTIFY

- NIST SP 800-171 CMMC
- FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems
- **DFARS 252.204-7012** Disclosure of Information
- **DFARS Case 2019-D041** Assessing Contractor Implementation of Cybersecurity Requirements



Design Tips for Cybersecurity & Resilience

- Invest in your cybersecurity workforce Security Engineering
- Design and plan for security updates and patches in your products
- Stay abreast of external system updates and patches Apply Them
- Provide allowances for future growth Network, IT Rack Space
- Incorporate DevSecOps Build Security into Products Upfront
- Perform Cyber Tabletop Exercises (TTX) What If's
- Document valid system operation, expected behavior PPSM
- Deny by Default Disable all unnecessary services
- Defense in Depth, Isolate your systems Slow down attacks





