# Cybersecurity and Cyberspace Operations

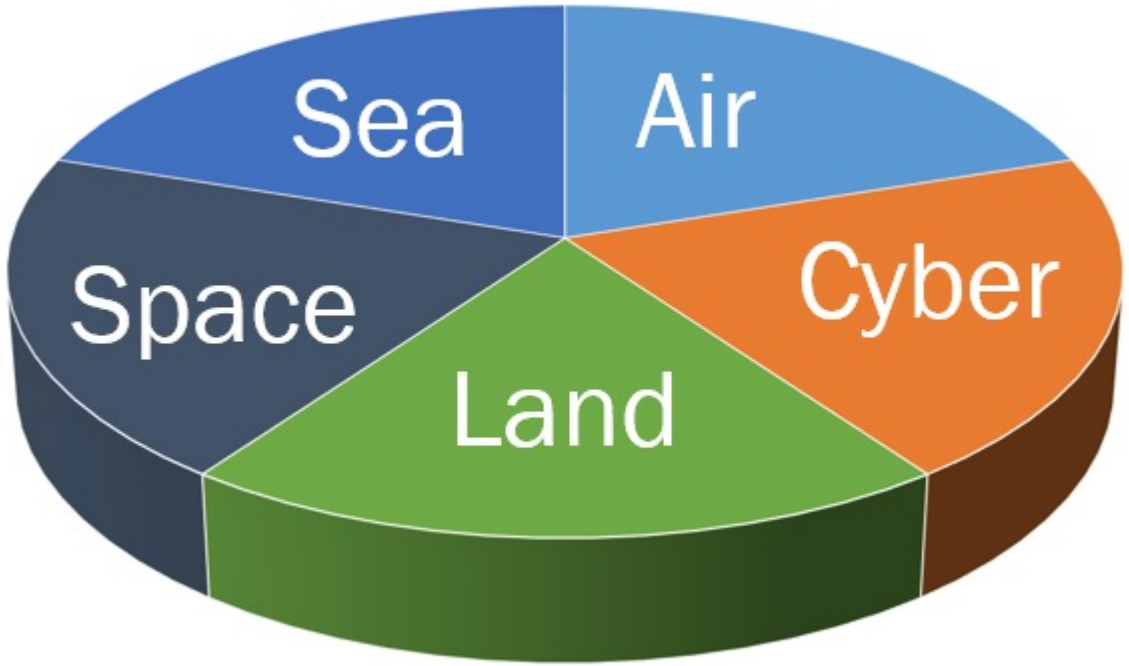
LCDR Steve Albert, USCG

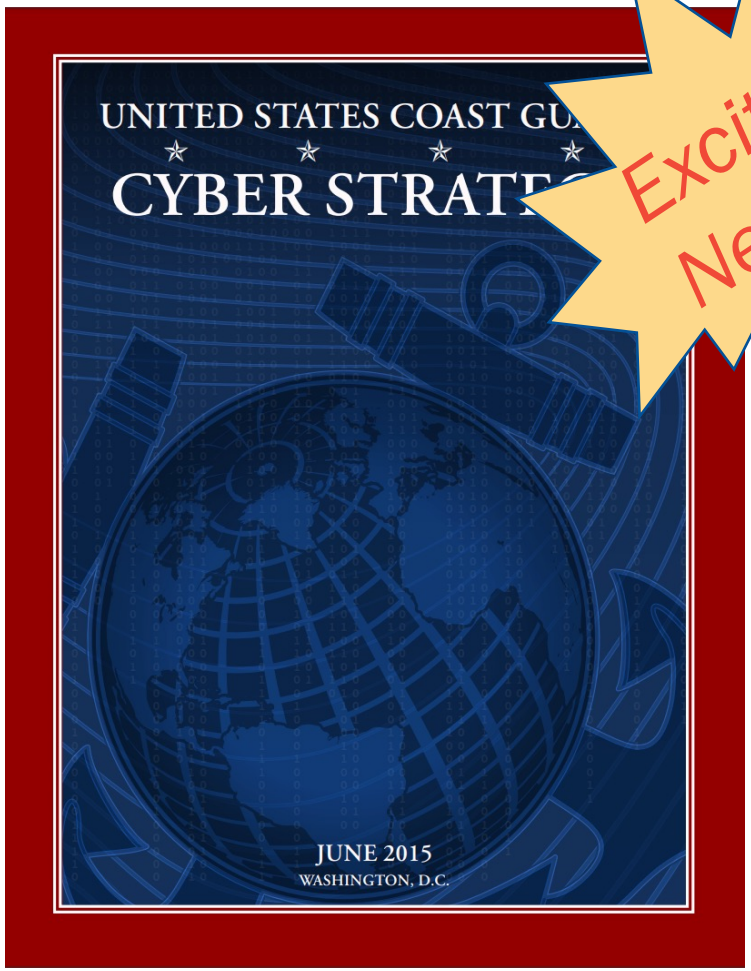
Office of Cyberspace Forces (CG-791)

Sea Air Space 2021

# Cybersecurity and Cyberspace Operations

# What is Cyberspace?




Exciting News!

# Why is Cyberspace Important?

**500+ ATTACKS**
Major technology cyber-attacks in the marine industry in 2020

**39 SECONDS**
Average time between daily hacker attacks

**36 BILLION**
Number of records exposed by data breaches in the first half of 2020

**$5.4 TRILLION**
Annual dollars estimated to travel through the MTS

**$10.5 TRILLION**
Estimated annual cost attributed to damage from cyber crime by 2025

# U.S. Coast Guard Cybersecurity and Cyberspace Operations






# Securing U.S. Coast Guard Cyberspace

NIST Framework for Improving Critical Infrastructure Cybersecurity


NIST SP 800-53

# 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*

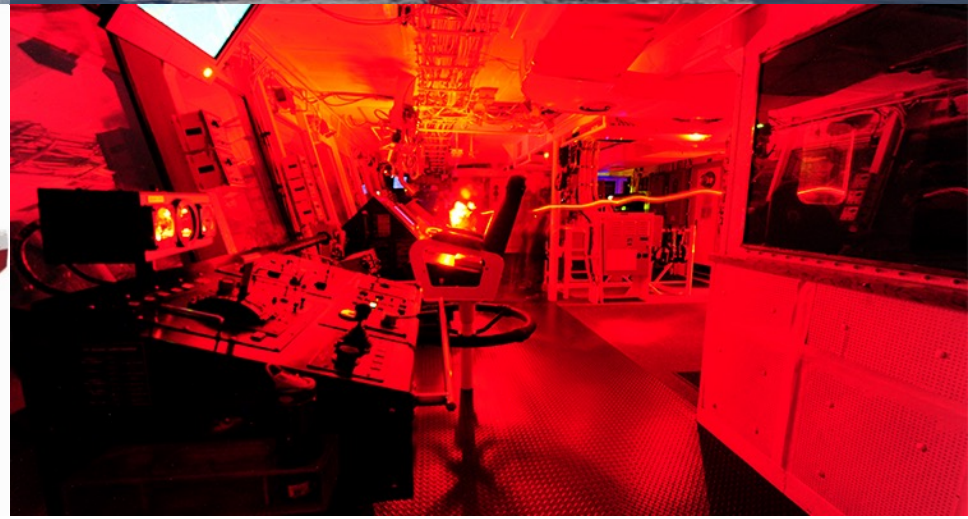
The U.S. Coast Guard will embed cyber planning in our traditional missions and plan to execute cyberspace operations that combine the Service's unique authorities, capabilities, and workforce to deliver mission success.

# Improving Acquisition Cybersecurity

# Valuable U.S. Coast Guard Cyber Targets

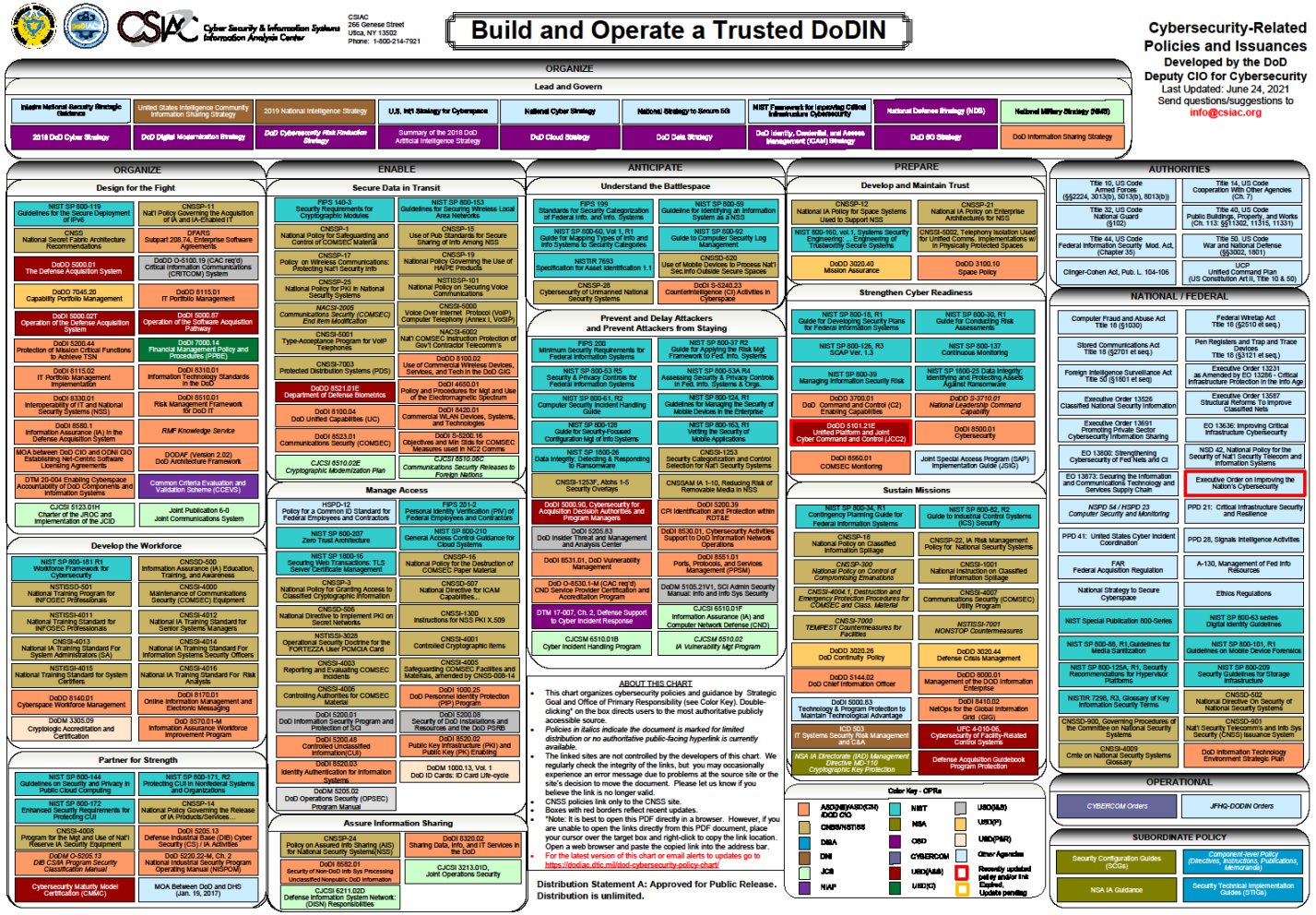




# Securing the Supply Chain

# Security Policy & Technology Familiarization

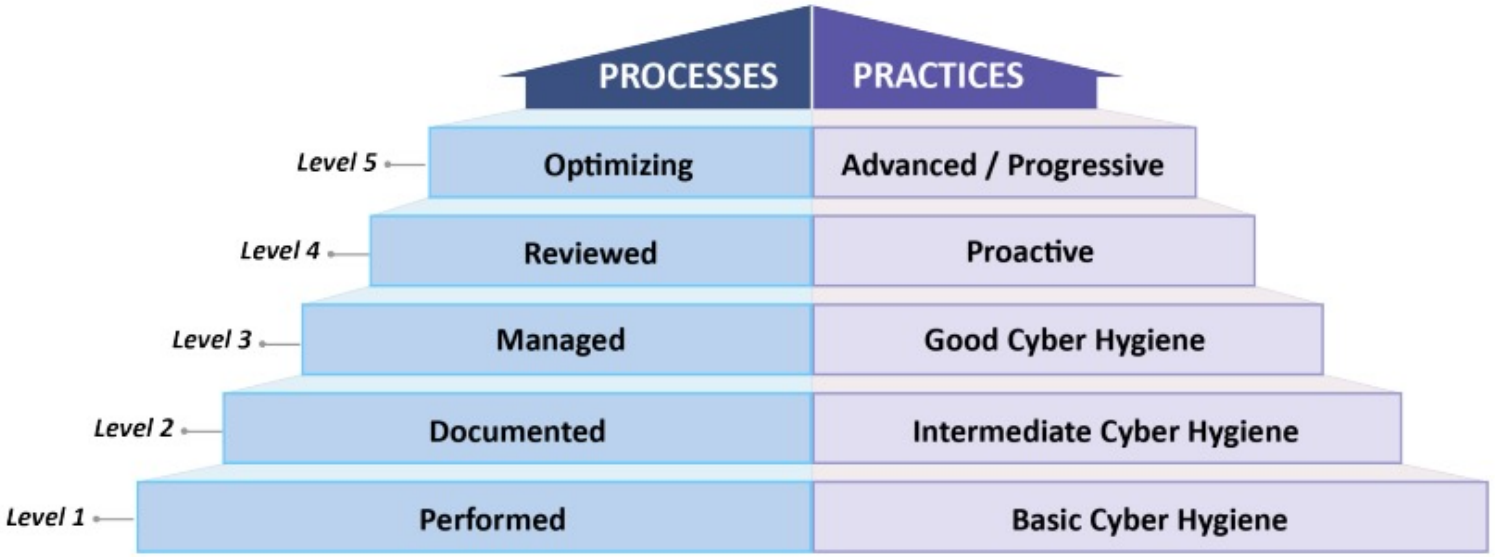



## DoD Cybersecurity Policy Chart

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

# Improve *Your* Organization's Cyberspace Operations

## Cybersecurity Maturity Model Certification (CMMC)



# Cyber Supply Chain Risk Management (C-SCRM)


- **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*

# Q&A