Strategic Intent for Cyber Ready

SECNAV Memo - Publish Date: 08/04/22

download PDF

This memo details how the DON will transform its approach to cybersecurity by pivoting from a compliance mindset to a dynamic model rooted in the philosophy of readiness and currency, called Cyber Ready.

SUBJECT: Strategic Intent for Cyber Ready

Reference: (a) Department of the Navy Information Superiority Vision, 14 Feb 2020

Enclosure: (1) Cyber Ready Description

For too long, the cybersecurity posture of the Department of the Navy (DON) has been based in a compliance approach that depends on checklists and policy to secure our technology. We have ample evidence over the past 15+ years that this approach is ineffective and cumbersome as was highlighted by the 2019 Secretary of the Navy Cybersecurity Readiness Review and commented extensively on in the press and Congress. Better cybersecurity is not achieved solely through compliance, and compliance-based approaches are insufficient to secure the DON.

In support of the DON's Information Superiority Vision (reference (a)), the DON will transform its approach to cybersecurity by pivoting from a compliance mindset to a dynamic model rooted in the philosophy of readiness and currency, called Cyber Ready, which is described in enclosure (1). This shift to a preemptive and active Cyber Ready state will improve the DON's cyber defenses while also speeding the process of acquiring cyber secure systems.

Within 30 days of this memorandum, the DON Chief Information Officer, Deputy Assistant Secretary of the Navy for Information Warfare and Enterprise Services, and Deputy DON Chief Information Officer (Navy and Marine Corps) will appoint leads and supporting organizations for each of the lines of effort described in enclosure (1).

We must change our cybersecurity approach to better compete in today's contested cyberspace. Cyber Ready promises significant improvements to DON's cybersecurity, but this complex, enterprise-wide change management effort will only succeed with the enthusiastic, fully committed support of many stakeholders, a well-developed, resourced and aggressively executed plan, effective oversight, and sustained senior leadership support. I am fully supportive of Cyber Ready and know you will be key contributors to this effort so important for the DON to maintain maritime dominance.

Signed by:
Carlos Del Toro

Enclosure: Cyber Ready Description

"Cyber Ready" is a continuous state of cybersecurity awareness, where the right to operate is earned and managed every day. A Cyber Ready posture ensures secure delivery of information into the right hands at the right time, through the acquisition and deployment of systems that are designed to be cyber secure.

Because our strategic adversaries leverage the cyber domain to erode our military, technological, and economic advantages, cybersecurity in the DON cannot be an afterthought. Instead, the Cyber Ready approach will be integral to the acquisition life-cycle from the beginning, which is only possible with a strong, enduring relationship between the acquisition and cyber communities. Cybersecurity requirements will be considered during design and systems engineering with embedded and transparent Cyber Ready approval processes synonymous with air and sea worthiness. Requirements developed with this approach will also account for the needs of both the warfighter for whom the capability is intended, and the cyber operators tasked to keep systems secure.

Both systems designed with cybersecurity from the beginning and those operating under the current compliance-based approach will transition to the continual state of Cyber Ready by achieving “Cyber Currency,” which is the set of standards that must be met for an ongoing authority to operate (ATO). Cyber Currency is based on demonstrating that personnel development/training and Cyber Ready requirements have been met. It is validated through favorable continuous monitoring (CONMON) results, metrics-based ongoing assessments, and adversarial testing.

To transition from the current compliance-based approach for cybersecurity to Cyber Ready, DON will pursue the following seven lines of effort.

1. Cyber Metrics: Measure cybersecurity holistically with a risk and readiness Zero Trust mindset.
2. Build on RMF Reform. Accelerate the ATO process with automation and leverage inheritance models to reduce the allocated control sets that programs are responsible and accountable for.
3. Cyber Currency; Move to an ongoing ATO that is maintained through Cyber Currency.
4. Adversarial Assessment. Adopt a “trust but always verify” mindset (leverage automated penetration testing, audits, and data from CONMON).
5. Data Analytics: Democratize insight by providing visibility into the Cyber Ready posture to those who need to know the risks they are assuming.
6. Acquisition Changes: Provide programs the tools to develop systems that are "born" Cyber Ready and remain ready through Cyber Currency.
7. Workforce: Deliver ongoing training to keep the acquisition and cyber workforce informed on the current processes and tools.

The LOE teams chartered by this memo will partner with stakeholders across the DON to produce deliverables in support of the Cyber Ready effort. Anticipated deliverables include, but are not limited to:

- Consistent risk assessment methodology;
- Establishment of a Cyber Ready approach over the system lifecycle;
- Acquisition process and tools to develop systems that are designed Cyber Ready and remain ready through Cyber Currency;
- Acquisition-led assessments and pilots of the Cyber Ready approach;
- Automated adversarial testing tools and other automation tools; and
- CONMON policy, which sets the minimum requirements for a system to achieve an Ongoing Authorization.

TAGS: CISO: Cybersecurity, Cybersecurity, IA, InfoSharing, Strategy, Workforce

Related Policy

Cybersecurity Awareness Month 2023

Adoption of NIST SP 800-53 and CNSSI 1253 Revision 5

US Navy Insider Threat Awareness Month

Strategic Intent to Implement Zero Trust

DON Enterprise Service Designation for Naval Integrated Modeling Environment

View More

Related News

The DON CIO is on LinkedIn

Apply Now to Demonstrate Solutions and/or Contributions to ISV 2.0 at the 2024 IT Conference East

Missed the 2024 DON IT Conference West?

Registration Open for 2024 DON IT Conference East

2024 DON IT Conference West Presentations Available

View More

Related CHIPS Magazine

Marines' experimentation with Joint Integrated Fires proves successful during Project Convergence Capstone 4

Official says commercial space strategy is driven by imperative to maintain warfighting edge

CISA announces Malware Next-Gen analysis

Secretary Del Toro releases Science and Technology Strategy, offers path for sustained innovation

USCYBERCOM: Fostering innovation and talent development

View More

Related Resources

Featured Articles: Oct - Dec 2023

Featured Articles: April - July 2023

Featured Articles: Jan - Mar 2023

Featured Articles: Oct - Dec 2022

2022 Cybersecurity Awareness Month Briefing Card - "See Yourself in Cyber"

View More