DEPARTMENT OF THE NAVY

CYBER STRATEGY

NOVEMBER 2023

THE SECRETARY OF THE NAVY
WASHINGTON DC 20350-1000

FOREWORD

The Department of the Navy's (DON) priority is strengthening maritime dominance in defense of the United States in line with the National Defense Strategy (NDS). The NDS lists defending the American homeland, paced to the growing multi-domain threat posed by the People's Republic of China (PRC), as our top defense priority. Alongside the physical domains, the Navy and Marine Corps must compete in cyberspace, defending American interests, enabling maritime dominance, and supporting integrated deterrence.

With the importance of the cyber domain in mind, I directed the DON Principal Cyber Advisor (PCA) and the DON Chief Information Officer (CIO) to draft a comprehensive cyber strategy ensuring the DON's cyber posture positions the naval services for success during competition, crisis, and conflict. The *Department of the Navy Cyber Strategy* describes how the DON will achieve the Cyberspace Superiority Vision and Information Superiority Vision for the full breadth of our cyberspace activities.

These efforts are an enduring strategic imperative for the DON. The 2019 SECNAV-directed Cybersecurity Readiness Review (CRR) – a comprehensive review of the DON's cyber readiness posture – demonstrated the urgency with which the naval services must mitigate cybersecurity risk and strengthen our prowess in cyberspace. In response, DON leadership empowered the DON CIO office, leading to the publication and implementation of the DON Information Superiority Vision. Relatedly, the DON PCA office was created in 2020 and quickly established a strong partnership with DON CIO, leading to the joint development of this strategy.

The *Department of the Navy Cyber Strategy* identifies seven distinct lines of effort the DON will undertake to enhance its cyber posture. In the spirit of "Get Real, Get Better," this strategy identifies numerous areas for improvement, outlining how the DON plans to double-down on successful initiatives and improve where required. In particular, this strategy will address enterprise cybersecurity, operational cyber defense, and offensive cyber operations. Understanding the critical role cyberspace plays in strategic competition, and recognizing the pace at which we must act, the DON CIO and DON PCA will identify governance forums that provide the oversight needed to ensure accountability and drive this strategy's execution.

I would like to thank all the DON personnel who contributed to developing this first ever *Department of the Navy Cyber Strategy*. The challenges inherent to the cyber domain are considerable, but failing to mitigate cyber risks is not an option. I am confident this strategy provides the DON with an effective roadmap to excel in cyberspace and compete with our adversaries on all fronts.

Carlos Del Toro

Carlos Del Toro
Secretary of the Navy

INTRODUCTION

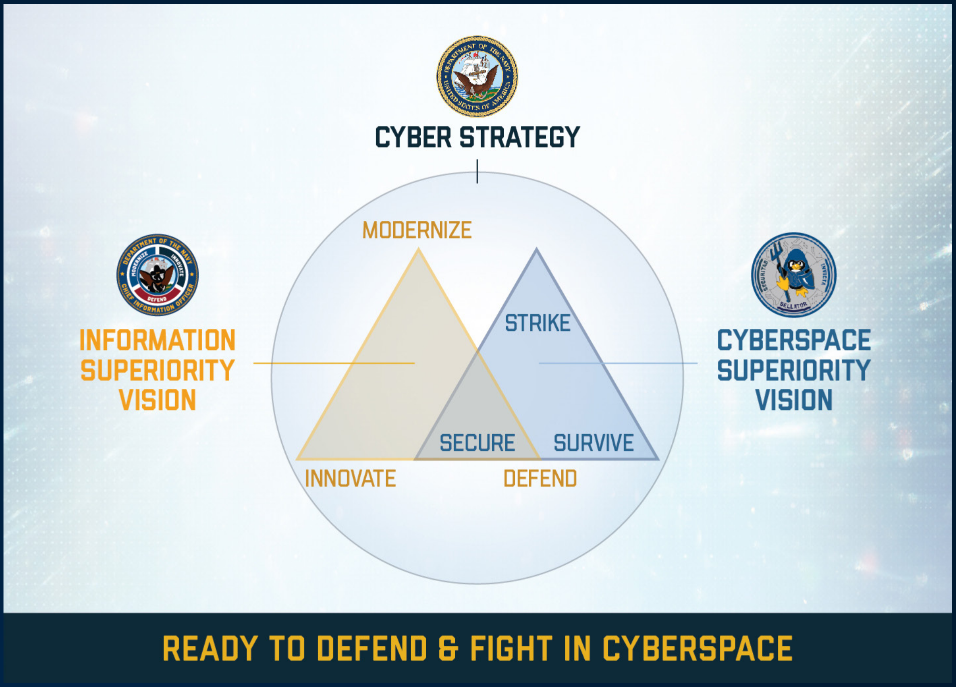
The next fight against our major adversary will be like no other in prior conflicts. The use of non-kinetic effects and defense against those effects prior to and during kinetic exchanges will likely be the deciding factor in who prevails. The side that most effectively sequences and synchronizes non-kinetic effects will have a decisive advantage. We must ensure our capabilities to project power and defend in cyberspace take top priority to ensure the success of the traditional power projection capabilities of our naval forces.

The Navy and Marine Corps cannot rely exclusively on traditional naval power in future maritime conflicts. While the foundational concepts of maritime warfare have not changed, we must fully account for new realities presented by cyberspace and the information environment. This requires embracing cyber and information warfare as core competencies for the naval services and recognizing their utility in maritime contexts. The actions we take – or neglect to take – during strategic competition directly impact our warfighting effectiveness, readiness, and ability to respond credibly to crises.

The DON requires a comprehensive strategy for defending and fighting in cyberspace that positions it to succeed at all levels of competition, crisis, and conflict. This strategy establishes specific lines of effort supporting the Department of Defense (DoD) Cyber Strategy and adhering to the tenets of the 2020 DON Information Superiority Vision (ISV) and the 2022 DON Cyberspace Superiority Vision (CSV).

The ISV and CSV's tenets serve as "north stars" for DON's cyberspace and information activities:

- The ISV calls for the DON to modernize its infrastructure, innovate and deploy new capabilities, and defend its information.
- The CSV calls for the DON to secure its systems, survive adversary cyberattacks through resiliency, and strike the adversary in and through cyberspace when required.


CYBER STRATEGY
MODERNIZE
STRIKE
INFORMATION SUPERIORITY VISION
CYBERSPACE SUPERIORITY VISION
SECURE
SURVIVE
INNOVATE
DEFEND
READY TO DEFEND & FIGHT IN CYBERSPACE

Relationships between the ISV, CSV and *Department of the Navy Cyber Strategy* are depicted in Figure 1.

The ISV articulates the foundational vision (modernize, innovate, defend) for the design and sustainment of the information technology and cyber infrastructure upon which offensive and defensive cyber operations will be launched. The CSV articulates the warfighting vision (secure, survive, strike) that integrates foundational IT capabilities, offensive and defensive cyber capabilities, and cyber workforce talent to protect defense critical infrastructure (DCI) and drive maritime competitive advantage in and through cyberspace.

The DON will execute a threat-informed, risk-based approach for prioritizing the most pressing lines of effort to achieve cyberspace and information superiority.

The DON will strengthen its collective efforts by assigning responsibilities and allocating needed resources through sustained governance and oversight. Our end state is a DON capable of fighting and winning in cyberspace and the information environment across the spectrum of conflict.

The Department of the Navy Cyber Strategy aligns directly to the National Security Strategy, National Cybersecurity Strategy, National Defense Strategy (NDS), and the DoD Cyber Strategy. It recognizes and accounts for the complex cyber and geopolitical security environment described in these policy documents, and it describes how the DON will implement higher strategic guidance in the naval services.

STRATEGIC ALIGNMENT WITH DEFENSE STRATEGY

The NDS outlines four defense priorities:

1	2	3	4
Defending the homeland, paced to growing multi-domain threats posed by the People's Republic of China (PRC).	Deterring strategic attacks against the United States, Allies, and partners.	Deterring aggression, while being prepared to prevail in conflict when necessary – prioritizing the PRC challenge in the Indo-Pacific region, then the Russia challenge in Europe.	Building a resilient Joint Force and defense ecosystem.

The DoD Cyber Strategy outlines four lines of effort:

1	2	3	4
Defend the Nation.	Prepare to fight and win the Nation's wars.	Protect the cyber domain with Allies and partners.	Build enduring advantages in cyberspace.

Recognizing the strategic environment described in the NDS, the naval services will advance and support defense priorities through integrated deterrence, campaigning, and building enduring advantages. The Department of the Navy Cyber Strategy focuses on the intersection of the maritime domain, information environment, and cyberspace to outline context-specific lines of effort and outcomes that enhance national security.

Integrated Deterrence

The NDS emphasizes deterrence by denial, resilience, and cost imposition as methods supporting integrated deterrence.

Deterrence by **denial** requires investments in mature, high-value assets while improving the integration of non-kinetic effects. Through zero trust architectures, defense-in-depth, modern cryptographic capabilities and enhancements, insider threat prevention, and defensive cyber operations, we can protect high-value assets required for denial strategies and prevent adversaries from undermining our advantages.

Deterrence by **resilience** – defined as the ability to withstand, fight through, and recover quickly from disruption – requires strengthening cyberspace defenses for priority networks, critical infrastructure, weapon systems, and platforms.

Finally, deterrence by **cost imposition** requires the development of credible offensive cyberspace and related non-kinetic capabilities to punish unacceptable adversary behavior when denial and resilience strategies are insufficient.

Campaigning

The NDS calls for strengthening deterrence and gaining military advantages through campaigning – defined as the conduct and sequencing of logically-linked military activities to achieve strategy-aligned objectives over time. This approach lends itself to cyberspace, where competitors constantly interact in an effort to shape the cyber strategic environment to their interests. To enable campaigning and set favorable conditions in cyberspace, the DON will present forces that can credibly conduct cyberspace operations to degrade competitors' malicious cyber activity. This includes preparing cyber capabilities to be used in crisis or conflict and tailoring their application to the maritime domain.

Building Enduring Advantages

The NDS requires building enduring advantages in numerous critical areas. The *Department of the Navy Cyber Strategy* helps build these advantages by focusing on technology modernization and innovation, civilian and military cyber workforce development, integrating cybersecurity into the acquisition process, and protecting the industrial base from cyber exploitation. Maintaining and enhancing these advantages positions the naval services to outpace our adversaries and remain competitive in an evolving security environment.

> **"We aim to deter cyber attacks from state and non-state actors and will respond decisively with all appropriate tools of national power to hostile acts in cyberspace, including those that disrupt or degrade vital national functions or critical infrastructure."**
>
> - **National Security Strategy,** October 2022

DRIVING CULTURAL CHANGE IN THE DEPARTMENT OF THE NAVY

Building a robust cyber culture is challenging and requires substantial time, resources, and effort. That said, it is essential for securing our information from compromise and enabling our activities in the physical domains. Creating this culture is a collective responsibility that must be embraced by all military, civilian, and contractor personnel.

A strong sense of cyber responsibility must pervade throughout the entire organization, from our newest recruits to our most experienced leaders. A sense of personal cyber responsibility must become an integral part of our values and principles, guiding our actions, and ensuring vigilance throughout the ranks.

To ensure future generations of Sailors and Marines understand cyber threats and their duty to protect the DON from intrusions, we will publish foundational guidance for all Sailors and Marines to learn during their initial officer and enlisted training. In this way, we will begin building a cyber culture from the ground up to complement our efforts to drive cybersecurity accountability at the highest levels of the naval services. Building this foundational understanding of our individual cyber responsibilities enables our successful application of the lines of effort outlined below.

LINES OF EFFORT

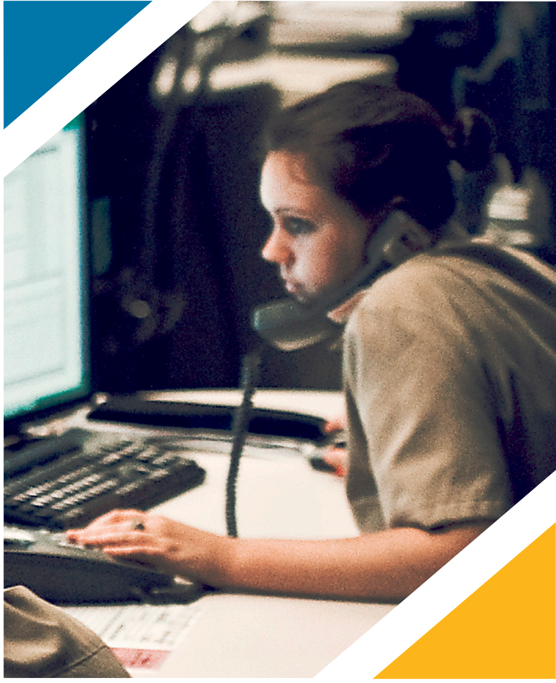
The following lines of effort detail how the DON will pursue information and cyberspace superiority in alignment with the DoD Cyber Strategy and NDS:

1. **Improve and Support the Cyber Workforce**
2. **Shift from Compliance to Cyber Readiness**
3. **Defend Enterprise IT, Data, and Networks**
4. **Secure Defense Critical Infrastructure and Weapon Systems**
5. **Conduct and Facilitate Cyber Operations**
6. **Partner to Secure the Defense Industrial Base**
7. **Foster Cooperation and Collaboration**

> **“When combined, a strong culture and thoughtful strategy become the key ingredients to execute efficiently and effectively as well as make and sustain meaningful change.”**
>
> - **Secretary of the Navy Cybersecurity Readiness Review,** March 2019

“Our most important cyber capability is people: those with the talent, creativity, and sense of mission necessary to defend the Nation in cyberspace.”

- **Department of Defense Cyber Strategy,** September 2023



1.0 Improve and Support the Cyber Workforce

Improving and supporting the cyber workforce is foundational to the success of this strategy. Without a robust, agile, and capable cyber workforce, the DON cannot make progress in improving our security, resiliency, or warfighting prowess in cyberspace. The following sub-lines of effort are designed to strengthen the cyber workforce and improve the DON's ability to recruit, develop, and retain best-in-class talent that can secure, operate, and defend the Department of Defense Information Network (DODIN). These sub-lines of effort will be augmented with other best practices developed by individual organizations but shared more broadly within an active, engaged cyber workforce functional community.

1.1 Improve recruitment efforts to attract the nation's top cyber talent

Our cyber workforce is critical to improving the DON's cybersecurity, resiliency, and warfighting capacity. To strengthen recruiting efforts, the DON will ensure commands have the information and incentives to fully use available hiring authorities like Cyber Excepted Service (CES) which improve recruiting and retention of civilian cyber talent. In addition to CES, the DON will promote a wider understanding of other recruiting tools, such as the direct hiring authorities available to hiring managers.

The DON will expand the Navy and Marine Corps' presence at career fairs, including university hiring events, to attract qualified talent. There are numerous internship and scholarship programs to attract college graduates, and we will ensure commands and hiring managers are fully aware of these opportunities. In addition, the DON will explore ways to identify promising new talent and attracting them, such as through Science Technology Engineering and Math (STEM) outreach programs, cyber competitions, and pre-accession cyber-proficiency testing.

The DON will strengthen relationships between technology organizations and the Office of Civilian Human Resources to leverage their recruiting talent, best practices, and recruiting advances as part of the DON's Civilian Human Capital Strategy.

1.2 Improve workforce management

The DON will implement the DoD Cyberspace Workforce Qualification and Management Program – in alignment with the DoD Cyber Workforce Strategy – to help assess and develop the workforce, build career paths, improve recruiting and retention, and support talent management initiatives. Additionally, we will develop and execute a plan to collect and analyze data to drive improvements in workforce planning, readiness, satisfaction, and human resource processes.

With respect to military talent management, the DON will evaluate different approaches to military recruitment and methods to increase career flexibility, then adopt recommendations deemed useful for the DON. In particular, we will explore innovative ways to recruit experienced civilian cyber talent and allow them to enter the naval services at positions commensurate with their experience.

1.3 Enhance cyber talent development

The DON will develop programs for internal mobility and career progression, allowing people to move more easily across roles and experiences within the DON. We will promote current and planned programs that offer rotational opportunities with industry and within DoD. We will also explore creative methods for assessing cyber aptitude of new talent and "in house" personnel interested in the cyber workforce. To foster capability advancement across all proficiency and experience levels, we will improve and expand new employee development programs and progressively build cyber capability in the workforce.

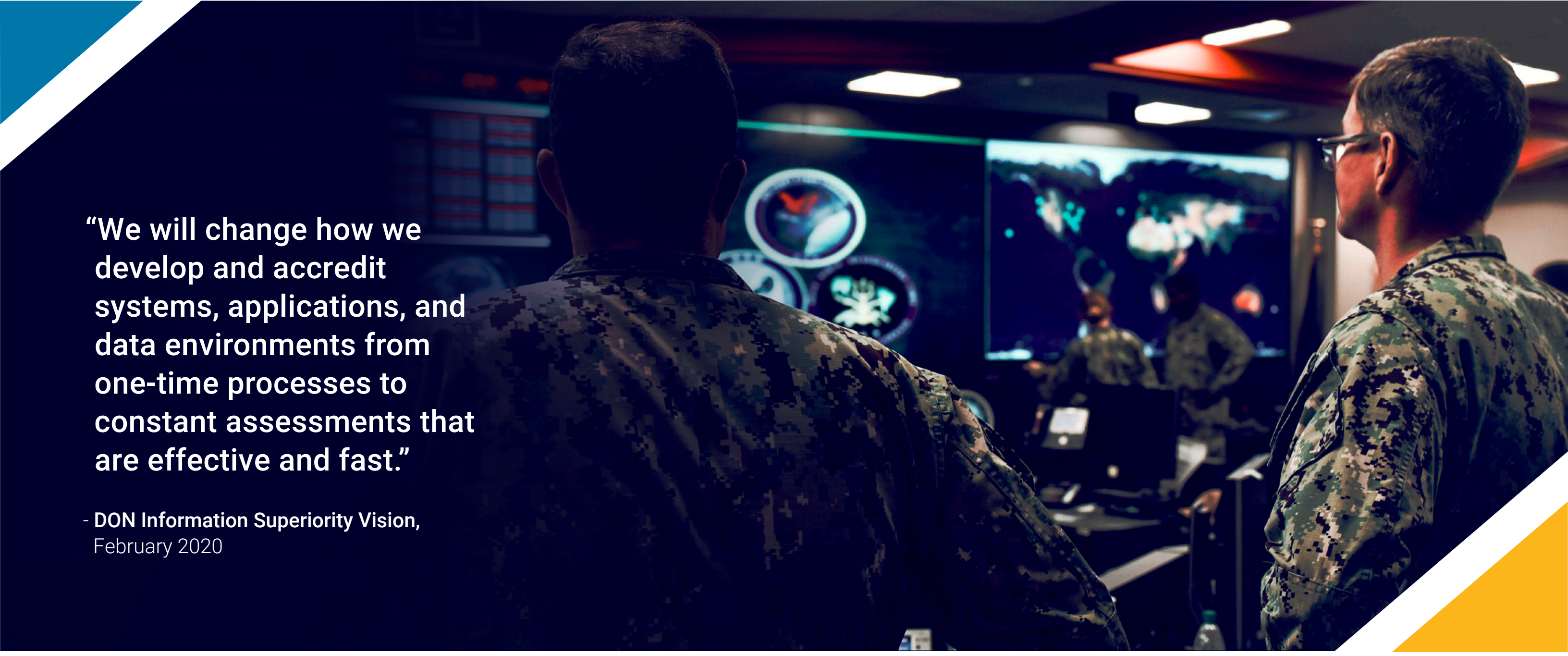
Relatedly, the DON will increase training options available to the cyber and non-cyber workforce, providing accessible, high-quality, and relevant training on digital learning platforms, and expand partnerships with academia and commercial vendors to provide certification, customized coursework, and degree options. The DON will also review other training and development alternatives to determine their applicability.

1.4 Strengthen retention efforts

The DON will ensure funding for the CES Targeted Local Market Supplement and other incentives for eligible work roles. In conjunction with existing pay incentives and promotion opportunities, the DON will offer non-traditional benefits, including flexible scheduling, assignment choice, and family benefits to retain its civilian cyber professionals. We will evaluate current military and civilian retention efforts to determine if changes are needed or if new initiatives are warranted. To remain responsive to the cyber workforce, the DON will solicit feedback from the cyber workforce through surveys and focus groups, and we will collect information from cyber professionals who leave the naval services to identify areas for improvement.

1.5 Promote cybersecurity awareness in the workforce

Although people are our greatest asset, any individual can represent a potential cyber vulnerability unless they practice sound cyber hygiene. Establishing a cybersecurity culture throughout the DON is an intentional process that begins with the DON leadership and extends to every individual in the enterprise. We will augment our existing practices to promote a cybersecurity culture with a sustained, robust cybersecurity information campaign. We will modify this campaign based on measures of effectiveness such as simulated phishing events, surveys, and breach analytics.



> “We will change how we develop and accredit systems, applications, and data environments from one-time processes to constant assessments that are effective and fast.”
>
> - **DON Information Superiority Vision,** February 2020

2.0
Shift from Compliance to Cyber Readiness

The DON needs a new approach to cybersecurity that goes beyond compliance because our over-reliance on compliance has resulted in insecure systems, which jeopardize the missions these systems support. Instead of a compliance mindset, the DON will shift to Cyber Ready, where the right to operate is earned and managed every day. The DON will make this transition by adhering to an operationally relevant, threat-informed process that affordably reduces risk and produces capabilities that remain secure after they have been delivered at speed. At the same time, the DON will institute changes that reduce the burden and improve the efficacy of compliance requirements. In pursuit of this line of effort, the DON will collaborate with relevant internal and external stakeholders to implement the following sublines of effort.

2.1
Measure risk consistently

The DON will measure cybersecurity holistically with a risk and readiness mindset by developing a consistent method of assessing cybersecurity risk.

2.2
Shift to a “cyber currency” mindset and democratize insight

The DON will move to a process that bases the right to operate on remaining current with Cyber Ready requirements (“cyber currency”). These requirements include continuous, near real-time monitoring of the effectiveness of security controls to the maximum extent possible, adversarial assessments, and cyber hygiene. How well systems meet these requirements will determine whether they are ready to be deployed or can continue to operate. Because cyber currency demonstrates cybersecurity readiness, it will be required for an ongoing Authority to Operate (ATO).

We will provide visibility into the cybersecurity posture, delivering decision-ready information through data analytics to the level of detail required by all relevant cyber professionals ranging from system administrators to senior leadership. This visibility will enable cyber professionals to understand the status of their networks and systems and the risks they are assuming, including mission impacts of these risks. Achieving this level of insight will require close collaboration between the acquisition and operational communities.

2.3
Conduct regular adversarial assessments

The DON will provide realistic risk assessments by conducting regular program-driven automated and manual testing of security protections from an adversary’s perspective. Findings from previous assessments will be reviewed to ensure remediation. Without frequent realistic assessments of its cybersecurity defenses, the DON risks operating with a false sense of security while overlooked weaknesses go unaddressed and missing valuable input that can assist with prioritizing mitigations and cybersecurity investments.

2.4
Make acquisition changes

For new systems, the DON will integrate cybersecurity into the earliest stages of development through design and systems engineering processes that make cybersecurity an integrated element of acquisition instead of a separate effort. Cybersecurity testing and validation will become an integral part of the software development process through Development, Security, and Operations (DevSecOps). The development process may also include other proven approaches for reducing software vulnerabilities. In close coordination with their Resource Sponsors and the operational community, program managers will utilize this Cyber Ready approach to deliver secure solutions and keep them secure over their lifecycles. The DON will make provisions to apply as much of the Cyber Ready approach as possible to legacy and joint systems, which will help them meet policy requirements to reduce cyber risk over the system lifecycle.

2.5
Prepare the workforce

The DON will provide training to cybersecurity practitioners, program managers and acquisition personnel so they understand how to incorporate cybersecurity into acquisition and adhere to new or updated policies, methodologies, procedures, processes, concept of operations, and management controls introduced by this shift to a Cyber Ready approach. The DON will also close any training gaps that keep operators and defenders from meeting cyber currency training and drilling requirements.

> “We will defend our information, wherever it is: at rest, in transit, or in external systems.”
>
> - DON Information Superiority Vision, February 2020

3.0 Defend Enterprise Information Technology IT, Data, and Networks

Defending enterprise IT, data, networks, and information systems is fundamental to deterrence by denial strategies, in addition to the secure pillar of the Cyberspace Superiority Vision and numerous priority areas outlined in the Information Superiority Vision. As the DoD Zero Trust Architecture Strategy states, our adversaries are in our networks, exfiltrating our data, and exploiting DoD users. To address this, the DON will pursue the following sub-lines of effort.

3.1 Identify and manage IT assets

The DON will increase automation and implement capabilities to provide ubiquitous, continual discovery and monitoring of all hardware, software, and IT services to better manage cybersecurity risks. We will mature our comply-to-connect solution that identifies systems connected to the enterprise network and ensures they are properly protected before granting access. We will extend this capability to non-enterprise networks.

3.2 Deploy innovative protection measures to safeguard our systems

The DON will implement Zero Trust and continue deploying Naval Identity Services – the DON’s identity, credential, and access management (ICAM) solution which supports Zero Trust. Until Zero Trust is fully implemented, and in environments where Zero Trust is not a viable option, we will protect against cyber compromise with defense-in-depth and segmentation and continue to apply defense-in-depth where appropriate.

We will reduce our attack surface by implementing security controls, divesting from duplicative IT infrastructure and support services, consolidating legacy networks, transitioning to enterprise IT services, de-duplicating non-authoritative data, and moving workloads and user productivity capabilities to the cloud.

In response to advanced cyber threats, we will deliver resilient software at speed by accelerating adoption of DevSecOps practices and integrating security at every phase of the software development lifecycle.

3.3 Rapidly detect cybersecurity incidents

To maximize the early detection of cybersecurity vulnerabilities and incidents, the DON will mature processes and solutions for detecting anomalies, improve threat intelligence, and develop more robust threat-hunting capabilities. We will further develop processes and solutions for logging network and system events, retain and manage log data, and leverage big data and artificial intelligence to visualize and address our most significant vulnerabilities and threats. To reduce the risk of insider threats, we will increase User Activity Monitoring coverage.

3.4 Quickly respond to cybersecurity incidents

The DON will develop and regularly test plans to respond to incidents. Testing will include simulated cyberattacks capturing relevant metrics to improve detection, analysis, and mitigation actions. As part of testing, the DON will assess whether sufficient personnel are available and properly trained to execute these plans within response standards. We will continue developing out-of-band management capabilities to improve command and control during normal operations and compromises.

> “Defending the systems and assets that constitute our critical infrastructure is vital to our national security, public safety, and economic prosperity.”
>
> - **National Cybersecurity Strategy,** March 2023

4.0
Secure Defense Critical Infrastructure and Weapon Systems

The Navy and Marine Corps depend on critical infrastructure to project power, sustain expeditionary operations, and effectively deter aggression through denial and resilience strategies. While our infrastructure was sufficient for military mobility in the absence of peer competitors, the realities of strategic competition require the DON to rapidly improve security and resilience benchmarks in line with the National Cybersecurity Strategy.

While critical infrastructure protection is an interagency endeavor, defending our weapon systems and warfighting platforms is a unique responsibility for the military and intelligence communities. We will double down on existing programs and initiatives that are producing results and focus near-term efforts on “bolting on” security and resiliency capabilities to deployed assets. For future platforms and weapon systems, we will increasingly “bake in” security from the beginning of a platform’s lifecycle and rebalance our acquisition priorities accordingly.

The following sub-lines of effort describe how we will **survive** adversary cyberattacks and strengthen security and resiliency for our critical infrastructure, weapon systems, and platforms.

4.1
Train personnel to respond, recover, and defend

The DON anticipates adversary forces will attempt to damage our critical infrastructure and weapon systems through cyberattacks. Therefore, everyone who works with these systems requires robust training and testing via simulations and exercises to effectively respond to and recover from cyberattacks, with some requiring more in-depth training than others. The ultimate goal is restoring system functionality and getting back into the fight. These processes are fundamental to strengthening the Navy and Marine Corps’ combat readiness and ensuring our ability to fight through disruption. In pursuit of this goal, the DON will develop and exercise immediate actions Sailors, Marines, and civilians must take in rapid response to cyberattacks on our infrastructure and weapon systems.

4.2
Expand visibility and security for operational technology and industrial control systems

To protect our critical infrastructure and weapon systems, the DON will map its mission-relevant terrain in cyberspace for Task and Defense Critical Assets. Defending these critical assets will require the DON to establish clear lines of responsibility for their defense, develop concepts of operation, have visibility of these systems, institute protections and redundancies, and ensure personnel assigned to defend critical infrastructure are appropriately trained, resourced, and funded. To ensure effective monitoring and response options, we will prioritize investments in capabilities that expand our situational awareness for industrial control systems.

4.3
Secure weapon systems and platforms

To improve weapon systems resilience, the DON will continue supporting the Strategic Cybersecurity Program and evaluate current weapon system security baselines and processes to detect, protect, and respond to cyberattacks. In line with the NDS, we will enhance cybersecurity and resilience for high-value assets to enable deterrence by denial strategies. Relatedly, we will prioritize investments in cyber capabilities that expand our situational awareness of OT and IT associated with weapon systems in addition to capabilities that enhance cyber boundary enforcement and cyber hardened operating environments. Finally, securing our weapon systems and platforms requires securing our information resident on industrial base networks, as described in line of effort 6.

4.4
Modernize and innovate to strengthen resiliency

Strengthening critical infrastructure resiliency often requires modernizing the underlying systems and technologies to enable the use of the latest cybersecurity tools. Therefore, the DON will modernize OT systems where appropriate to enable the application of cutting-edge cybersecurity defenses. Where system modernization is not possible, the DON will use innovative solutions to improve system resiliency and work around constraints resulting from legacy hardware.

4.5
Leverage emerging technologies

Emerging technologies such as quantum computing and artificial intelligence present tremendous “leap ahead” cybersecurity opportunities. For all IT systems, we will stay abreast of emerging commercial technologies that can help improve our cyber defenses, and quickly adopt the most promising solutions. We will partner with the research and development community and commercial partners to share our cybersecurity requirements, evaluate solutions, pilot capabilities, provide feedback, and transition the best solutions to operations. With the right combination of rapid experimentation opportunities, policy considerations, incentive structures, and risk tolerance, existing investments can accelerate and scale the most promising and beneficial emerging capabilities.

"We will conduct cyberspace operations to degrade competitors' malicious cyber activity and to prepare cyber capabilities to be used in crisis or conflict."

- **National Defense Strategy,** October 2022

5.0 Conduct and Facilitate Cyber Operations

Cyber operations are an increasingly important component of modern statecraft and the Navy and Marine Corps require cyber forces and capabilities to successfully campaign and impose costs on malicious actors. Developing effective, reliable, responsible, and controllable cyber capabilities is an intentional process that requires significant time, resources, and personnel. Relatedly, cyberspace operations forces cannot be trained overnight, and there are substantial challenges maturing our cyber forces. We will focus time and resources on the following sub-lines of effort to position the Navy and Marine Corps to exploit advantages inherent to the cyber domain.

5.1 Present capable cyber forces

The DON will man, train, equip, and resource capable cyber forces for combatant commanders to deliver warfighting effects in and through cyberspace. This includes creating the Cyber Warfare Technician rating and the Maritime Cyber Warfare Officer designator. In addition, we will work closely with combatant commanders to determine critical personnel requirements for the most useful and needed forces and utilize emerging training environments to reduce any training backlog. Importantly, these forces must operate at a high level of readiness to respond dynamically to adversary activity and set the conditions to achieve cyberspace superiority.

5.2 Provide credible cyber capabilities

The NDS calls for preparing cyber capabilities for use in crisis and conflict. This requires balancing the acquisition of cyber tools from industry with the development of boutique "in-house" cyber capabilities. Internal capability development requires robust and sustained investments to effectively transition the most promising capabilities from research and development into the hands of operators. Although we must conceal these capabilities, our operators also must understand how to employ them when called upon. To that end, we will develop and enhance state-of-the-art cyber training environments while leveraging currently available joint training solutions. In addition, we will ensure cyberspace capabilities and their associated effects are integrated into military war games, simulations, and exercises to gain experience weaving these capabilities into traditional operations.

5.3 Contribute to the development of joint cyber warfighting platforms

Our Sailors and Marines will soon rely on joint platforms to deliver effects in and through cyberspace. Therefore, the DON will contribute to the development of emerging cyber warfighting platforms and adopt and comply with joint cyber architecture standards to accelerate cross-Service threat intelligence sharing. The DON's participation ensures the considerable knowledge and experience of our Sailors, Marines, and civilians will improve the development process for these joint platforms and guarantee their interoperability with current Navy and Marine Corps systems and capabilities.

5.4 Integrate non-kinetic effects

Although cyber capabilities can provide significant value on their own, they are most effective when combined with related capabilities. Mixing and matching the correct combination of non-kinetic effects – including cyber, electronic warfare, and information operations – typically generates outsized operational utility compared to standalone uses. To take advantage of these combined capabilities, the naval services must account for non-kinetic effects in strategic plans, budgeting, acquisition, orders development, and execution. Our forces require these blended non-kinetic capabilities at the tactical edge to support fleet operations and provide "on-net" cyber operators with "off-net" access via physical proximity. To this end, the Navy will explore the development of Service-retained teams operating at a high level of readiness to execute these missions and deliver value to the force.

"It is unthinkable to cede the maritime, air, or land domains to adversaries without a fight, and the DON must view cyberspace in the same way. We must dynamically project power in and through cyberspace as part of integrated deterrence."

- **DON Cyberspace Superiority Vision,** October 2022

6.0 Partner to Secure the Defense Industrial Base

The DoD DIB Cybersecurity Strategy outlines numerous lines of effort for hardening DIB networks and protecting sensitive data. Notably, nearly every line of effort requires coordination and collaboration between key stakeholders to produce results. Accordingly, the following sub-lines of effort are designed to drive a holistic approach to DIB cybersecurity and promote collaboration between the DON and industry partners.

6.1 Harden the DIB

In partnership with the DIB and other stakeholders, we will promote and develop innovative, active measures to improve the security of DON data safeguarded by the DIB and improve our visibility of how well industry partners are protecting our data in their systems. The DON's preference will be for solutions that provide real-time protections and insight and the DON will work with Federal stakeholders to identify ways of simplifying compliance frameworks without sacrificing cybersecurity. The DON will support useful programs and initiatives in other organizations when possible, such as the National Security Agency's Cybersecurity Collaboration Center, DoD Cyber Crime Center (DC3), and Naval Criminal Investigative Service (NCIS) programs.

6.2 Warn the DIB

The DON plays an important role in disseminating cyber threat information to the DIB, and we will work with relevant Federal agencies to make other threat intelligence available to our DIB partners. The DON will encourage participation in voluntary threat sharing programs and also promote commercial solutions that alert DIB participants to detected threats.

6.3 Report DIB Compromises

The DON will support DoD efforts to quickly report DIB compromises, and we will improve the process of notifying operational commanders when DIB data associated with critical technologies is compromised. Clear standard operating procedures for reporting cyber intrusions will alert the chain-of-command more quickly and enable stakeholders to respond promptly in coordination with the affected entity.

6.4 Strengthen Contracts

Incorporating strong cybersecurity language into contracts is key for DIB partners to secure DON data resident on their systems. The DON will team with acquisition stakeholders to ensure DIB cybersecurity contracts require statements of work containing the enhanced security controls language necessary to ensure robust cybersecurity practices.

6.5 Partner with the DIB

To maintain situational awareness, solicit ideas, gather feedback, and, ultimately, better defend DON data and supply chains, we will continue developing and fostering relationships with DoD, industry partners, suppliers, and other DIB stakeholders while expanding the group of contractors we regularly engage with now. We will continue information sharing initiatives and look for other opportunities to promote awareness of other Secure the DIB initiatives. As a strategy, the DON will focus on critical programs and technology and then primarily on small and medium size entities, which do not have the resources of large prime contractors, to ensure they are aware of support structures for protecting their own and the DON's information.

6.6 Reduce supply chain cybersecurity risks

We depend on supply chains for products and services that enable the DON to achieve its strategic and operational objectives. To strengthen the resilience of our supply chains, the DON will identify supply chain risk and implement cybersecurity risk management controls, processes, and activities across the system development lifecycle commensurate with the criticality of supplied products and services for a cost-effective, risk-based approach.

> "We will invest in rapid information-sharing and analysis and will develop a comprehensive approach for the identification, protection, detection, response, and recovery of critical DIB elements, thereby ensuring the reliability and integrity of critical weapons systems and production nodes."
>
> - **Department of Defense Cyber Strategy,** September 2023

7.0 Foster Cooperation and Collaboration

Cyberspace is a global and extraterrestrial domain that requires effective partnerships to master. The DON is not alone in promoting American interests in the cyber domain, and we can leverage existing and emerging partnerships to improve our activities in cyberspace. Cooperation and collaboration support all lines of effort in this strategy. In addition to driving internal cooperation and collaboration within the DON between the Secretariat, Navy, and Marine Corps, we will engage the following external partners and tailor our relationships appropriately.

7.1 Promote cooperation with Federal stakeholders

Prevailing in the cyber domain requires close coordination between Federal agencies. The DON will continue to coordinate with other Military Services as well as the Office of the Secretary of Defense. We will also partner with relevant stakeholders outside DoD such as Congress, other Executive Branch agencies, including key players in cybersecurity such as the Department of the Homeland Security, and the Intelligence Community, and other stakeholders. Information sharing is critical to reducing our shared attack surface, responding to cyber incidents, establishing sound policies and procedures, and promoting a shared understanding of cybersecurity risks to our enterprise.

7.2 Interface with non-governmental entities

Non-governmental entities experience many of the same cybersecurity challenges faced by the DON. Threat information sharing with commercial entities, academia, and other non-governmental entities is critical to enhancing cybersecurity. Where possible, the DON will explore technical exchanges with non-governmental entities and pursue information sharing initiatives to improve situational awareness in cyberspace. We will also identify commercial and non-commercial products to augment our cyber capabilities. Furthermore, the DON will support existing U.S. government programs that seek to improve cybersecurity information sharing between the governmental and non-governmental entities. Similarly, the DON will double down on academic partnerships and facilitate academic exchanges, internships, and collaborative research on cybersecurity.

7.3 Leverage alliances and partnerships

Every nation contends with cyber threats and brings their own experiences to the table. We will identify areas for cooperation between the DON and other agencies in allied and friendly governments, including through the North Atlantic Treaty Organization, Five Eyes, and other international structures. We will engage with Allied and friendly nations to exchange best practices, share appropriate information, and coordinate our efforts in cyberspace.

> “The Department will maximize its effectiveness in cyberspace by combining its efforts with those of Allies and partners.”
>
> - **Department of Defense Cyber Strategy,** September 2023

ACCOUNTABILITY, OVERSIGHT, AND EXECUTION

Given the importance of the cyber domain and knowing that swift action is needed, the CIO and PCA will work with the Navy and Marine Corps to identify governance forums that provide the oversight needed to meet the desired outcomes of this strategy. These forums will prioritize implementation, assign roles and responsibilities, monitor progress, and measure outcomes.

CONCLUSION

The *Department of the Navy Cyber Strategy* contributes to the defense of the nation and enables the sustainment of American sea power. Alongside our efforts supporting maritime dominance in the physical domains, we must develop and build on our capabilities in cyberspace to enable naval operations and structure our forces for success in strategic competition. These actions are fundamental to defending the free and open rules-based order that has generated unprecedented prosperity, interconnectivity, and freedom for decades. To advance our defense priorities, the DON must concurrently **modernize** our infrastructure, **innovate** rapidly, **defend** our information, **secure** our systems, **survive** adversary cyberattacks, and present forces and capabilities to **strike** in and through cyberspace.

GLOSSARY

Cyber Hygiene – The use of cybersecurity controls in an operational environment to prevent successful attacks on cyber networks, computers, and application by adversaries with minimal capability and intent. (DoDI 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers, 31 December 2020)

Cyber Ready – A strategic DON initiative for improving its cyber defenses by pivoting from a compliance mindset to a dynamic model rooted in the philosophy of readiness, where the right to operate is earned and managed every day. Cyber Ready will integrate cybersecurity into the development process and continuously monitor, assess and report on the DON's cybersecurity posture.

Cybersecurity Supply Chain Risk Management – A systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. (NIST SP 800-161r1)

Cyberspace – A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)

Cyberspace Operations — The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Also called CO. (JP 3-0)

Cyberspace Superiority — The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force and its related land, air, maritime, and space forces at a given time and place without prohibitive interference. (JP 3-12)

Cyberspace Workforce – Personnel who build, secure, operate, defend, and protect DoD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations; and project power in or through cyberspace. It is comprised of personnel assigned to the following workforce elements: IT, cybersecurity, cyberspace effects, intelligence workforce (cyberspace), portions of the Intelligence workforces and cyberspace enablers. The Data Analyst and Database Administrator work roles are part of the IT workforce element. (DoD Directive 8140.01)

Defense Critical Asset – An asset of such extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its missions. (DOD Directive 3020.40 CH1)

Defense Critical Infrastructure — Department of Defense and non-Department of Defense networked assets and facilities essential to project, support, and sustain military forces and operations worldwide. Also called **DCI**. (JP 3-27)

Defense Industrial Base — The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development and design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. Also called **DIB**. (JP 3-27)

Defensive Cyberspace Operations — Missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. Also called DCO. (JP 3-12)

Development, Security, and Operations – A software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops). The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of software development: plan, develop, build, test, release, deliver, deploy, operate, and monitor. (DoD Enterprise DevSecOps Fundamentals)

Industrial Control System – General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy). (NIST Special Publication 800-82, Rev 2 – Guide to Industrial Control System Security)

Information Environment – The aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information. Also called IE. (JP 3-04)

Information Superiority – The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (Department of the Navy Information Superiority Vision)

Information Technology – Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. (40 U.S.C. § 11101(6))

Offensive Cyberspace Operations — Missions intended to project power in and through cyberspace. Also called OCO. (JP 3-12)

Operational Technology – Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. (NIST Special Publication 800-37 Revision 2)

Task Critical Asset – An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD or OSD Components to execute the task or mission-essential task it supports. TCAs are used to identify DCAs. (DOD Directive 3020.40 CH1)