



# Department of the Navy Information Superiority Vision



**February 2020**

Page Intentionally Blank



THE SECRETARY OF THE NAVY  
WASHINGTON DC 20350-1000

February 14, 2020

FOREWORD

Information management, digital modernization, and the technology tools that enable them must be elevated as core strategic priorities across the Department of the Navy (DON). Cyber security, data strategy and analytics, artificial intelligence, and quantum computing have all combined to create massive opportunities and vulnerabilities across our entire enterprise. A critical element of mission readiness is our ability to access agile, reliable, and secure global communications and information, from the network enterprise to the tactical edge.

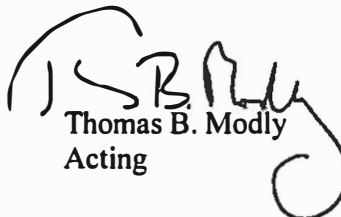
That is why we consolidated Department-wide information management strategy and functions into a restructured and empowered Office of the Chief Information Officer (CIO) led by Mr. Aaron Weis. Mr. Weis left a successful career as CIO in the private sector because he was drawn to our mission and he likes big challenges. He came to the right place! Under his leadership, the DON is executing a unified vision driving transformation and operational capability. If we are going to win tomorrow's fights, we must ensure operationally relevant information is in the right hands, at the right time. We need all hands on deck to execute the following three lines of effort of our new Information Management Strategy:

**Modernize** – We will modernize the DON infrastructure from its current state of fragmented, non-performant, outdated, and indefensible architectures to a unified, logical modern infrastructure capable of delivering information advantage. We will design a performant, defensible cloud-enabled, network leveraging robust identity management.

**Innovate** – We will use technologies like 5<sup>th</sup> Generation wireless and Artificial Intelligence to maximum effectiveness, and field new operational capabilities. We will create Digital Innovation Centers to accelerate software development and leverage best practices in the private sector and industry to fuel our digital transformation.

**Defend** – We will employ continuous active monitoring across the enterprise to increase cyber situational awareness and institute a security culture where a personal commitment to cybersecurity is required to gain access to the network. We will transform the compliance centered culture to one where security is constant readiness. We will work with our defense industrial base partners to secure naval information regardless of where it resides.

Everyone in the DON enterprise must become a Cyber Sentry. The more advanced we become as an Information-Based organization, the more our adversaries will seek to attack and exploit us in this domain. We will not be able to stop them unless everyone does their part to protect the advantages digital information provides, and limit the vulnerabilities it creates.

  
Thomas B. Modly  
Acting

# TABLE OF CONTENTS

---

<b>1</b>	<b>Introduction.....</b>	<b>1</b>
<b>2</b>	<b>Current situation.....</b>	<b>2</b>
2.1	Manual information integration – by the warfighter.....	2
2.2	Complex networks – our adversaries’ attack vector.....	2
2.3	Outdated processes and training corrode our information workforce.....	2
<b>3</b>	<b>Vision: Build Information Superiority to win the global naval fight .....</b>	<b>3</b>
3.1	The right information in the right hands, ready to decide, act, and fight .....	3
3.1.1	Discovery & Analysis – Generating Information Power .....	3
3.1.2	Delivery & Defense – A Constant State of Information Readiness.....	3
3.1.3	Decision & Action – Information is Combat Power .....	3
3.2	Modern, unified, and agile network .....	4
3.2.1	Modernized Network – Unified transport and upgraded infrastructure .....	4
3.2.2	Cloud processing and storage – unified shore and tactical edge afloat networks.....	4
3.2.3	User identity – unified across the DON .....	5
3.3	An Information Age workforce – a culture of Information Readiness .....	5
3.3.1	Continuously Learning, Always Advancing .....	5
3.3.2	Ready to fight tonight in cyberspace – Every Sailor, Marine, and civilian a cyberspace sentry.....	5
3.3.3	Actively, constantly audit ourselves to maintain our “Right to Operate” .....	5
3.3.4	The Information Environment as a critical part of all Navy and Marine Corps career paths .....	5
<b>4</b>	<b>How: Way forward.....</b>	<b>6</b>
4.1	Modernize our Infrastructure .....	6
4.2	Innovate and deploy new capabilities .....	6
4.3	Defend our Information.....	6
<b>5</b>	<b>Conclusion .....</b>	<b>7</b>
<b>6</b>	<b>Appendix I: Driving Competitive Advantage Overview .....</b>	<b>8</b>
<b>7</b>	<b>Appendix II: DON Information Superiority Vision Alignment.....</b>	<b>9</b>
<b>8</b>	<b>Appendix II: References .....</b>	<b>10</b>

Page Intentionally Blank

# 1 INTRODUCTION

---

*“The basic objectives and principles of war do not change. The final objective in war is the destruction of the enemy’s capacity and will to fight, and thereby force him to accept the imposition of the victor’s will.” – Admiral Chester W. Nimitz<sup>i</sup>*

War is intrinsically unpredictable. We reduce the fog of war by gathering information. We increase the enemy’s friction by creating uncertainty. In maneuver warfare, a commander masses distributed forces to decisively engage the enemy’s critical vulnerabilities to remove his center of gravity. Success depends on rapidly understanding the environment and enemy to make decisions faster than the adversary.

As stated by General David H. Berger, the 38th Commandant of the Marine Corps<sup>ii</sup>, the character of warfare has changed. Peer competitors operate in the grey zone. Adversaries gain an advantage in the Information Environment by leveraging a proliferation of inexpensive information technologies while developing high-tech capabilities for the kinetic fight. Success in traditional warfighting domains now requires mastering the Information Environment, which includes the electromagnetic spectrum, space, cyber domain, and the data that crosses them. Rapid data-enhanced decision-making, which increases lethality, defines warfare in the Information Age.

As an Information Age military, every warfighting function and mission area entirely depends on information and rapid decision-making throughout the entire competition-conflict continuum. The SECDEF highlighted information’s critical nature by establishing it as the 7th Warfighting Function. **Information is Combat Power.**

Information Superiority is delivering the right information to the right hands, ready to observe, orient, decide, and act faster than the adversary. It provides freedom of action within the Information Environment for friendly forces and prevents interference by the opposing force. As noted by Admiral Michael M. Gilday, the 32<sup>nd</sup> Chief of Naval Operations, in the Design for Maintaining Maritime Superiority, our Fleet will be a potent, formidable force that competes around the world every day, deterring those who would challenge us while reassuring our allies and partners. Commanders must maintain decision-making superiority and expand our digital competitive advantage.

Our National Defense Strategy mandates our focus on lethality, mission partners, and reform. The Navy and Marine Corps must set the conditions to master our information.

- First, we must **modernize**. By unifying and upgrading our networks, critical infrastructure, and processes, we settle our technical debt.
- Second, we must **innovate**. Leveraging emerging technologies, we transform our networks into a cutting-edge Information Age warfighting platform.
- Third, we must **defend**. The entire DON must continuously integrate defensive measures into processes, technologies, and our workforce.

We have the watch. We must think differently. Our mission is to build a more agile, innovative naval digital warfighting platform our leaders can leverage anytime and anywhere. We must modernize, innovate, and defend our information to achieve a digital edge that no adversary can match.



## 2 CURRENT SITUATION

---

The Department of the Navy (DON) lacks a mastery of its Information Environment. Our peer competitors desire to disrupt our ability to conduct battle by denying and degrading our means of sensing, understanding, and acting with coherency. The DON's current networks, associated processes, and culture compound the problem. Our networks limit access to data and fail to support efficient decision-making. Our antiquated systems are inadequate for the security environment described in the National Defense Strategy.

### 2.1 MANUAL INFORMATION INTEGRATION — BY THE WARFIGHTER

The DON's current networks and systems fail to deliver modern user experience, and many users work around the network to accomplish their jobs. Simple capabilities such as file sharing, cloud collaboration, chat, voice, and video are not available to DON users. Forward-deployed Sailors and Marines must manually contextualize raw data from multiple unintegrated systems. The DON needs a network capable of delivering actionable information to the point of need.

### 2.2 COMPLEX NETWORKS — OUR ADVERSARIES' ATTACK VECTOR

The DON operates antiquated network structures designed in the 1990s, which limit access to critical information. Our adversaries gain an advantage in cyberspace through guerilla tactics within our defensive perimeters. They leverage phishing attacks, whaling attacks, and privilege escalation to gain access to our rear area. Once inside, malign actors steal, destroy, and/or modify critical data and information. The point of infiltration is often not the target location. As technology changes, our network no longer forms a linear battlespace simply defended by a Maginot line of firewalls. We must realize a unified and simplified network from ship to shore that integrates with joint and mission partner networks while creating hostile terrain for our adversaries.

### 2.3 OUTDATED PROCESSES AND TRAINING CORRODE OUR INFORMATION WORKFORCE

The DON faces challenges recruiting, developing, retaining, and employing an effective information workforce. Our checklist-based security culture, outdated information systems, and industrial age processes stifle innovative thinking and give a false sense of security. Many talented Sailors, Marines, and civilians move on from the DON to roles that offer more development and growth opportunities, access to leading technologies, and higher compensation. This loss requires the DON to import outside talent to senior positions rather than educate and develop the next leaders from within.

Our outmoded industrial age processes cannot solve information age problems. To unlock the future, our approach to our systems and networks must change. As we chart a course to **modernize**, **innovate**, and **defend** our information systems, we must cultivate and empower our workforce to successfully execute the unique and inspiring mission of the Navy and Marine Corps.

### 3 VISION: BUILD INFORMATION SUPERIORITY TO WIN THE GLOBAL NAVAL FIGHT

---

Future global naval conflicts will take place afloat, ashore, and in the Information Environment. Our network and platforms must allow us to evolve, grow, and adapt to out-cycle our adversaries – maneuver warfare in and through technology. The DON must securely deliver the right information to the right Sailor or Marine at the right time to defeat high-paced and evolving threats. As we adopt a model that allows us to **modernize**, **innovate**, and **defend** our platform, we unlock this future. The network itself becomes a warfighting platform.

#### 3.1 THE RIGHT INFORMATION IN THE RIGHT HANDS, READY TO DECIDE, ACT, AND FIGHT

The DON network, our naval digital warfighting platform, must autonomously deliver the right information to the right hands, ready to observe, orient, decide, and act. The DON's modernization efforts, aligned to the DOD Digital Modernization Strategy, must free humans to compete, fight, and win.

##### 3.1.1 Discovery & Analysis – Generating Information Power

Collecting and effectively categorizing data enables timely, accurate, and complete insights. Data tagging, storage, and visibility strategies provide the best-practices needed to develop usable information. Artificial Intelligence can analyze and contextualize massive amounts of data, freeing Sailors and Marines from repetitive machine-oriented tasks, and focusing cognitive effort on using the resulting information to achieve decisive effects.

##### 3.1.2 Delivery & Defense – A Constant State of Information Readiness

The network must securely deliver decision-ready information into the right hands at the right time to enable lethality. The network must protect data from interception, exfiltration, and corruption. Information Readiness requires caching of mission-critical data forward at the tactical edge and sharing situational awareness with higher headquarters to enable a near-seamless Information ecosystem.

##### 3.1.3 Decision & Action – Information is Combat Power

As we increasingly trust our algorithms, we move from humans identifying and classifying every target to approving target classifications (human in the loop), and finally to verifying automated classifications (human on the loop). This automation increases the speed at which warfighters can absorb information, make decisions, and act. *Automation will not replace the cognitive responsibility of humans to choose to engage.*



## 3.2 MODERN, UNIFIED, AND AGILE NETWORK

The DON must design the network's user experience to allow the warfighter to orient on the situation rapidly. It must provide properly credentialed Sailors and Marines access to information to fight from anywhere. We achieve this vision through one, logical, software-defined network leveraging elastic compute infrastructures, identity management, and modern software development. It must support contingency Command and Control situations. We defend this network layering security around our critical information.

### 3.2.1 Modernized Network – Unified transport and upgraded infrastructure

Information should be able to flow seamlessly, whether between business systems, readiness information systems, the tactical edge, and afloat networks. The network transport layer must enable this seamless flow of information.

#### *3.2.1.1 Simplify and unify our global network to make it easier to manage and defend*

The DON needs to re-envision, re-architect, and re-deploy our unclassified, classified, and top-secret networks to fully take advantage of the advances of the past 20 years. The DON network should function even in a denied, degraded, intermittent, and latent (DDIL) environment.

#### *3.2.1.2 Create Naval Mesh to change how we use information in the Fight*

We must leverage the existing Naval Tactical Grid (NTG) efforts to create a Naval mesh network extending the tactical edge organically without forward infrastructure. This mesh extends the DON network and, in DDIL environments, operates cut off from the DON network until connections are reestablished. The mesh scales from the large weapons platform of a Guided Missile Destroyer afloat to the individual Marines operating forward, connected by orbiting aerial platforms, existing military satellites, future low earth orbit (LEO) platforms, landlines, or other existing and emerging network nodes. These self-forming networks must operate with all the qualities of the DON network and organically form and de-form as needed, with associated access to any information (when not DDIL) through the seamless DON network.

#### *3.2.1.3 Bandwidth-rich environment that supports new capability*

As we move to the cloud, we will require more bandwidth to move increasingly large amounts of information between the tactical edge and enterprise. We must maximize this bandwidth-rich environment to prepare for times of limited connectivity – broken or degraded either by choice or through the adversary's actions. While we train to operate in a DDIL environment, we should leverage bandwidth opportunistically to make the most of connectivity when available. Also, we need to prepare on thin-line connectivity, and our architecture must accommodate any scenario, from seamlessly connected to entirely disconnected.

### 3.2.2 Cloud processing and storage – unified shore and tactical edge afloat networks

As the seamless, unified, logical network becomes a reality and Sailors and Marines move around the network with one unified identity, it will become possible for the tactical edge networks to operate within the one logical construct. Within this construct, tactical edge cloud devices that can operate in a DDIL environment will be able to seamlessly integrate to create operational edge capability.

#### *3.2.2.1 Design and Package for Deployment*

Capability must be usable by deployed warfighters. Deployment across DDIL environments, in cloud-ready packaging, will allow the capability to be deployed in days, not months or years.

#### *3.2.2.2 Build or Buy Once, Use Often (conservation of energy)*

We must avoid building on the DON's rich history of building duplicative information systems. We should use systems from the DOD or other DOD military services if they readily integrated into our network. We must conserve energy by building operational capabilities as efficiently and effectively as possible. We must embrace the same DevSecOps practices that enable our counterparts in industry to deploy new capabilities at speed, without sacrificing security or usability in the process.

#### **3.2.3 User identity – unified across the DON**

In the future, one unified identity must follow an individual from “hire to retire.” The DON must consolidate identity management systems to one unified system and identity per Sailor, Marine, or civilian. The DON must expand on the new Navy ERP and integrate with the DOD IDAM solution(s). Unified identity is a cornerstone of other technologies such as Zero Trust Architecture (ZTA). The DON IDAM solution should leverage the vendor architectures we currently operate.

### **3.3 AN INFORMATION AGE WORKFORCE – A CULTURE OF INFORMATION READINESS**

The DON must develop a transformative workforce ready to **modernize**, **innovate**, and **defend** our information.

#### **3.3.1 Continuously Learning, Always Advancing**

The DON needs to accelerate innovation by creating an ecosystem of Digital Innovation Centers. These innovation centers will bring together teams of Sailors and Marines to develop software solutions through user-centered design in DevSecOps with known tools and libraries. Each Innovation Center will share its solutions enterprise-wide, avoiding the redundancy of multiple teams “relearning” the same lessons.

**3.3.2 Ready to fight tonight in cyberspace – Every Sailor, Marine, and civilian a cyberspace sentry**  
“Every Marine a Rifleman” remains a core Marine Corps tenet. In today's security environment, we must instill the same discipline in cyberspace: “every Sailor, Marine, and civilian a cyberspace sentry.” We must remain vigilant every day from boot camp to retirement.

#### **3.3.3 Actively, constantly audit ourselves to maintain our “Right to Operate”**

By deploying a continuous audit capability, the DON “auto-red teams” our systems, Sailors, Marines, and civilians on their mastery of information defense. If we find vulnerabilities, we take corrective action, no different than grounding an aircraft or welding a ship to the pier. Verification and validation never end. Security becomes a state of being and readiness.

**3.3.4 The Information Environment as a critical part of all Navy and Marine Corps career paths**  
Information Environment training must be embedded through all levels and competencies, from basic ratings to post-graduate degrees. We must weave the Information Environment into every Sailor, Marine, and civilians' career paths, educational opportunities, and exposure to advanced technology. We need to fast-track and promote from below the zone for Sailors and Marines who excel in needed technical specialty areas. The DON's information environment and related processes must encourage innovative thought and build a culture of information exploitation infused into operations.

We must start building our future leaders today. Our future leaders need to come from within. The future DON CIO is a junior Sailor, Marine, or civilian today.

## 4 HOW: WAY FORWARD

---

In order to set ourselves on the path to gain Information Superiority, we will organize around three straightforward premises: modernize, innovate, and defend.

### 4.1 MODERNIZE OUR INFRASTRUCTURE

We will modernize the DON to a unified, logical infrastructure. The DON networks will need to transform with governance and resource structures. The DON will continue to modify acquisition practices to fully leverage leading edge technologies. Steps have been taken, but more needs to be done to consolidate cloud brokers, develop acquisition teams, and leverage agile development methodologies and partners. We cannot modernize in place. The DON will leverage the best practices of industry to lay down a new network foundation and migrate to it.

### 4.2 INNOVATE AND DEPLOY NEW CAPABILITIES

Innovation at the speed of relevance will allow new operational capability to be rapidly built, integrated, accredited, and deployed. The DON needs to build on the successes of in-house efforts around Compile to Combat in 24 Hours (C2C24) and NavalX, as well as efforts such as the N1 Transformation and the Air Force Kessel Run programs. Innovation should rapidly ingest new technologies to create capability. For AI, the DON needs to scale AI in partnership with the Joint AI Center (JAIC) to optimize the analysis phase of information management. Millimeter wave technology should be leveraged to extend the logical DON transport networks to the tactical edge, in coordination with the NTG program and to operate the NTG in DDIL environments. Other emerging technologies will continue to come on the scene and the DON needs to be ready to rapidly ingest those that are usable into the Innovation cycle.

### 4.3 DEFEND OUR INFORMATION

We will Defend our Information, wherever it is: at rest, in transit, or in external systems. In order to increase our information defense capability, we will continuously audit our employees and systems to move away from manual checklist based security. We also will change how we develop and accredit systems, applications, and data environments from one-time processes to constant assessments that are effective and fast. Finally, we will engage our Tier 1 Defense Innovation Board (DIB) companies to incentivize, support, and aid the Tier 2/3 companies to dramatically increase their security posture. Industry is part of the weapon system.

## 5 CONCLUSION

---

Developing Information Superiority will be no small feat. In addition to the technical challenges of updating and migrating the enterprise infrastructures and capabilities across the DON, there will be other critical elements that must be addressed in order to be successful.

We will think about how we previously governed our large enterprise infrastructures and how that contributed to our current state. As we **Modernize, Innovate, and Defend**, we will make adjustments that create accountability and drive action in short time frames. We will build on our past working relationships and discover ways to further drive transformation. We will manage our capabilities as a true enterprise portfolio. We will vigilantly nurture efforts that bear fruit and terminate unproductive efforts. We will work together to achieve these outcomes and avoid delays due to existing equities and “rice bowls”. We must align ourselves under a unified vision that makes the DON fully accountable to all of its personnel, to our stakeholders, leadership, and the American taxpayers.

Transformation for competitive advantage will never be “done”. We will embark on a journey where we never arrive at a destination but are always looking to leverage the next emerging technology or capability. We will constantly adjust how we defend the DON’s information in the face of ever-evolving adversaries.

Our ability to successfully execute and implement a comprehensive DON-wide, Information Superiority Vision will take a team effort. We will reach out across the DOD and whole of government, as well as to Congress, industry, and academic partners to move ourselves at the speed of relevance. We will build on others’ achievements.

This is a strategic initiative. This will require us to strive valiantly. The journey will be difficult and long – the credit belongs to the warrior in the arena. We must harness every advantage from our data, systems, technology, and capabilities. There is nothing more important than ensuring our Sailors, Marines, and civilians have every advantage to fight the adversary.

## 6 APPENDIX I: DRIVING COMPETITIVE ADVANTAGE OVERVIEW

UNCLASSIFIED



# DRIVING COMPETITIVE ADVANTAGE

*Build Information Superiority to Win the Naval Fight*

**MODERNIZE  
INNOVATE  
DEFEND**

**BRING THE DON  
INFRASTRUCTURE  
TO PARITY WITH  
INDUSTRY**

**DRIVE CAPABILITY  
OUTCOMES FOR  
COMPETITIVE ADVANTAGE,  
AT SPEED**

**DEFEND FORWARD WITH  
ROBUST INFORMATION  
PROTECTION**

**ACHIEVING  
OUTCOMES**

**NAVAL MESH  
(5G, TACTICAL  
GRID,  
NETWORKS)**

**FULLY LEVERAGE  
CLOUD/JEDI**

**WARFIGHTER**

**FULLY LEVERAGE  
ARTIFICIAL  
INTELLIGENCE**

**FLAT, DEFENDABLE,  
PERFORMANT NETWORK**

**BRING THE DON  
INFRASTRUCTURE TO  
PARITY WITH INDUSTRY**

**STANDARD CAPABILITY  
ACROSS PLATFORMS,  
MANAGED AS A  
PORTFOLIO OF SERVICES,  
AT SPEED**

**CRR REFORM ACTIVITIES**

**DEFEND FORWARD WITH  
ROBUST INFORMATION  
PROTECTION  
CONTINUOUS  
(MONITORING PHISHING,  
AUTO-RED-TEAM)**

**SECURE, OPTIMAL  
SUPPLY CHAIN AND  
LOGISTICS THAT  
ENABLES READINESS  
(CMCC, LEGISLATION)**

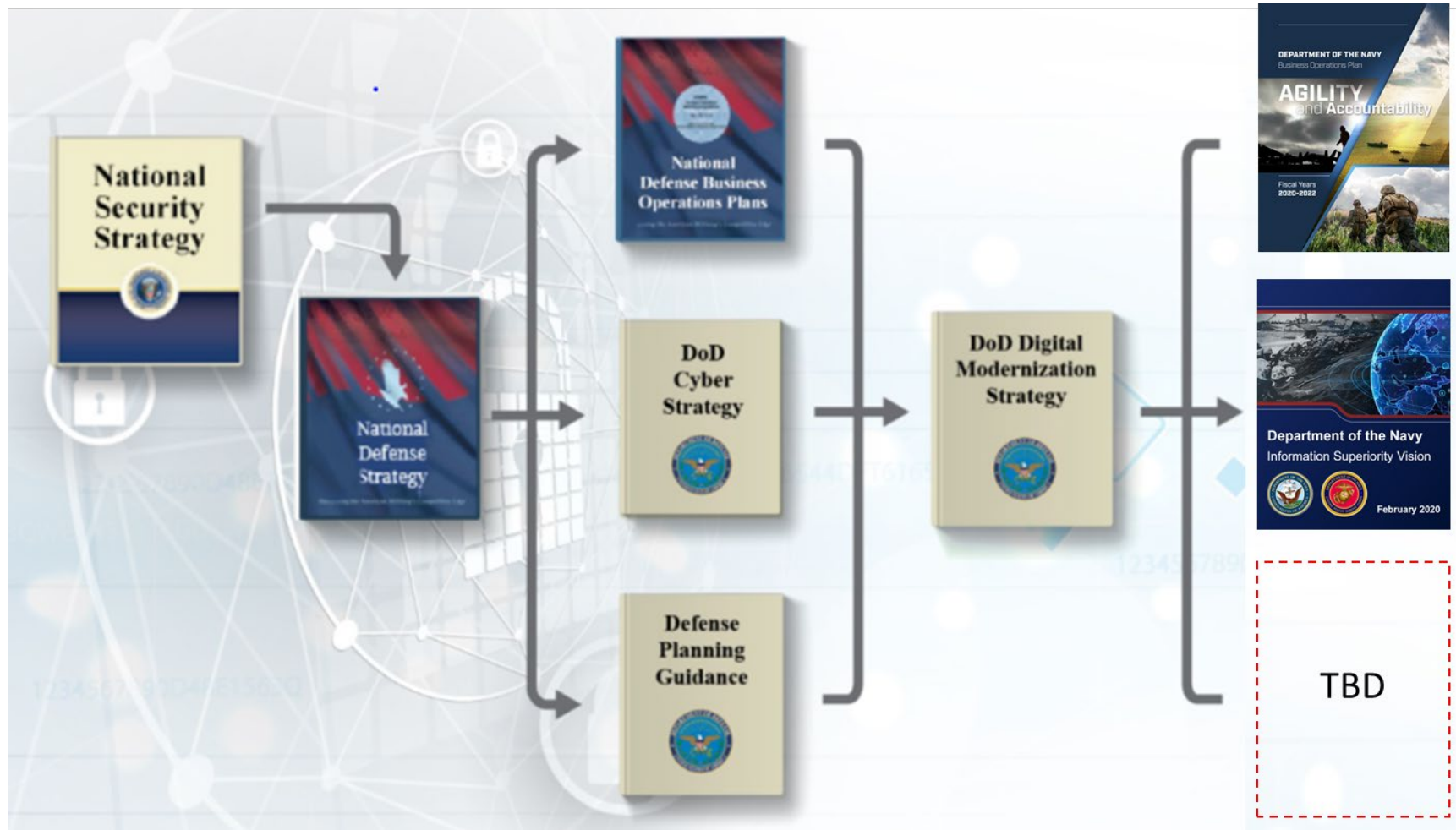
**"RIGHT TO OPERATE"  
MENTALITY,  
CYBERSECURITY AS A  
CONSTANT STATE  
(CYBER SENTRY)**

**CYBER EMPOWERED  
WORKFORCE  
(11 CYBER GENERAL  
ORDERS, CYBER  
EXCEPTED RECRUITING)**

**SINGLE IDENTITY  
ACCESS SOLUTION  
THAT INTERFACES WITH  
DOD**

UNCLASSIFIED

## 7 APPENDIX II: DON INFORMATION SUPERIORITY VISION ALIGNMENT



## 8 APPENDIX II: REFERENCES

---

<sup>i</sup> An essential task assigned by Admiral Chester W. Nimitz in Employment of Naval Forces (1948)

<sup>ii</sup> Townhall comments by General David H. Berger, the 38th Commandant of the Marine Corps in October 2019