Exhibit R-2, RDT&E Budget Item Justification: PB 2025 Navy											Date: March 2024	
Appropriation/Budget Activity 1319: *Research, Development, Test & Evaluation, Navy I* BA 6: *RDT&E Management Support*					R-1 Program Element (Number/Name) PE 0606355N *I Warfare Innovation Management*							
COST ($ in Millions)	**Prior Years**	**FY 2023**	**FY 2024**	**FY 2025 Base**	**FY 2025 OCO**	**FY 2025 Total**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2029**	**Cost To Complete**	**Total Cost**
Total Program Element	0.000	41.422	37.340	50.652	-	50.652	52.257	52.990	53.928	55.034	Continuing	Continuing
0798: *Allied/Coalition Maritime Environment (ACME)*	0.000	1.229	7.317	7.189	-	7.189	7.367	7.385	7.409	7.564	Continuing	Continuing
2144: *Space & Elec Warfare Engineering*	0.000	26.729	15.167	28.698	-	28.698	29.605	30.061	30.663	31.281	Continuing	Continuing
3319: *Fleet Experimentation*	0.000	11.060	12.346	12.338	-	12.338	12.761	12.975	13.235	13.513	Continuing	Continuing
3320: *TRIDENT Warrior*	0.000	2.404	2.510	2.427	-	2.427	2.524	2.569	2.621	2.676	Continuing	Continuing

A. Mission Description and Budget Item Justification

Allied/Coalition Maritime Environment (ACME) 0798:
This project promotes interoperability with allied and coalition forces by facilitating maritime interoperability in both processes and communication systems, including emerging capabilities, to counter growing high-end asymmetric threats.

Space & Electronic Warfare (SEW) Engineering 2144:
This project is a systems engineering non-acquisition program to develop, test, implement Technical Authority (TA) products, and validate Naval Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), Business Information Technology (IT), and Space System architectures to support naval, joint and coalition missions across normal, contested, and degraded cyber/operational environments. The objective of this project is performed through multiple tasks that ensure development and delivery of Naval Information Warfare (IW) capabilities that are well integrated, interoperable, secure, and resilient to meet validated warfighting requirements.

NAVWAR leads SECNAV guidance under Cybersecurity Technical Authority (CSTA) to define and employ a uniform objective recursive approach employing Cyber Ready strategy shifting away from a compliance only methodology. Efforts will automate program engineering reviews and speed IW capability certification and authorization to overmatch our adversaries in a Cyber contested environment.

Fleet Experimentation 3319:
The U.S. Navy's Fleet Experimentation (FLEX) project advances operational and tactical warfighter capabilities through the experimentation of high payoff initiatives, technologies and concepts, Fleet Concepts of Operations (CONOPS), doctrine, and new tactics, techniques and procedures (TTP). The main focus of FLEX between 2023 and 2028 is to operationalize A Design For Maintaining Maritime Superiority Blue Line of Effort (LOE) through the execution of Fleet Design materiel/non-materiel capability employment.

Trident Warrior Project 3320:

Exhibit R-2, RDT&E Budget Item Justification: PB 2025 Navy	Date: March 2024
Appropriation/Budget Activity 1319: *Research, Development, Test & Evaluation, Navy I* BA 6: *RDT&E Management Support*	**R-1 Program Element (Number/Name)** PE 0606355N *I Warfare Innovation Management*

The U.S. Navy's Trident Warrior (TW) experimentation campaign enables early delivery of capabilities to the warfighter via Fleet-directed Trident Warrior operational events with an emphasis on United States Fleet Forces/Commander Pacific Fleet (USFF/CPF) directed focus areas.

B. Program Change Summary ($ in Millions)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Previous President's Budget	52.060	37.340	39.520	-	39.520
Current President's Budget	41.422	37.340	50.652	-	50.652
Total Adjustments	-10.638	0.000	11.132	-	11.132
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-9.484	0.000			
• SBIR/STTR Transfer	-1.154	0.000			
• Program Adjustments	0.000	0.000	11.406	-	11.406
• Rate/Misc Adjustments	0.000	0.000	-0.274	-	-0.274

Change Summary Explanation

Increase in FY25 from previous President's Budget primarily attributed to Proj 2144 Space & Elec Warfare Engineering: FY25 increased by $11.693M to fully restore to prior year levels to support increased requirements for Enterprise Architecture, DON CISO Cyber Figure of Merit (CFOM) acquisition gate assessments, system of systems Cyber Risk to Mission (CRTM) assessments, Risk Management Framework (RMF) reform efforts to develop and advance the Continuous Monitoring (CONMON) and cyber operational picture capability required to meet Fleet Cyber Command (FCC) objectives. Increase also supports NAVWAR Digital Transformation efforts, system and system of systems model-based analysis, and the evolution of cybersecurity compliance activities.

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy			Date: March 2024
Appropriation/Budget Activity 1319 / 6	R-1 Program Element (Number/Name) PE 0606355N / *Warfare Innovation Management*	Project (Number/Name) 0798 / *Allied/Coalition Maritime Environment (ACME)*	

COST ($ in Millions)	Prior Years	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
0798: *Allied/Coalition Maritime Environment (ACME)*	0.000	1.229	7.317	7.189	-	7.189	7.367	7.385	7.409	7.564	Continuing	Continuing
Quantity of RDT&E Articles		-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The ACME program advances Information Warfare (IW) to include Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR); Electronic Warfare (EW); and Cyber Warfare, interoperability with Australia, Canada, New Zealand, United Kingdom, United States (AUSCANNZUKUS), North Atlantic Treaty Organization (NATO), and other Allied and Coalition partners. The program determines maritime operational gaps with our allies, identifies Doctrine, Organization, Training, Material, Leadership, Personnel, and Facilities (DOTMLPF) solutions with the potential to fill those gaps, and assesses these solutions and associated concepts of operation in laboratory and at-sea environments. The ACME program includes integration and testing in support of joint and Allied war fighting capabilities, including interoperability testing of IW equipment. Allied and joint interoperability is critical for future maritime operations, especially as the United States Navy cooperatively works towards a federated environment through initiatives such as Mission Partner Environment/ NATO Federated Mission Networking (MPE/FMN), Secret and Below Releasable Environment (SABRE), and U.S. Battlefield Information Collection and Exploitation System - eXtended (BICES-X).

Currently, IP connectivity with AUSCANNZUKUS and other Allied/Coalition forces is focused on traditional paths, requiring extensive backhaul through ashore infrastructure. Higher bandwidth solutions suitable for use over tactical networks require development and assessment for emerging coalition and joint interoperability requirements, such as Network Operations Without Shore (NOWS), Denied, Degraded, Intermittent and Low-bandwidth (DDIL) operations, and to counter Anti-Access Area Denial (A2/AD) threats. Increases in data throughput are required for the effective exchange of rich IW data sets and services via Service Oriented Architectures (SOA) within the limitations of High Frequency (HF), Ultra-High Frequency (UHF), and other portions of the radio frequency spectrum, coupled with appropriate Information Assurance and Computer Network Defense (IA/CND) mechanisms. Development and assessment of potential solutions will integrate improved IP capabilities with the Advanced Digital Network Systems (ADNS) and existing international standards (e.g. Allied Communications Publication 200, NATO Standardization Agreements 5066 and 4691). The continued development and refinement of advanced tactical networking technologies and protocols, to include Low Probability of Intercept (LPI), Low Probability of Detection (LPD), and Anti-Jam (AJ) capabilities as well as Automatic Link Establishment (ALE) standards, will provide for a significant improvement in secure data sharing within, and between, coalition maritime elements.

Coalition Warrior Interoperability eXperiment (CWIX) has been integrated with the ACME Program starting in FY24. CWIX efforts are focused on assessing federated Coalition capabilities within the NATO command construct via connected Live, Virtual, Constructive (LVC) capabilities resident in the Combined Federated Battle Laboratories Network (CFBLNet). CWIX also resources engineering activities in cooperation with PEO C4I to integrate USN Expeditionary Mission Partner Environment with US Air Force (USAF) Mission Partner Capabilities Office (MPCO) Enterprise Mission Partner Environment efforts. Additionally, CWIX resourcing enables assessment of NATO Federated Mission Networking Spiral Specifications as they relate to USN Programs of Record via the Coalition Interoperability Assurance and Validation (CIAV) construct in conjunction with Joint Staff J6.
Australia, UK, US (AUKUS) Electronic Warfare (EW) efforts have been integrated starting in FY24. Specific efforts focus on: Threat Assessment, Blue Force Data Analysis, Tactical Data Movement, Effects optimization, and Scenario development in Synthetic Environments.

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606355N / *Warfare Innovation Management*	**Project (Number/Name)** 0798 / *Allied/Coalition Maritime Environment (ACME)*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Title: Advanced Relay Capabilities	1.229	7.317	7.189	0.000	7.189
Articles:	-	-	-	-	-
FY 2024 Plans: - Australia, United Kingdom, United States (AUKUS) Electronic Warfare (EW) experiment planned for execution in RIMPAC 24 with a focus on Distributed Maritime Operations - Execute Coalition Warrior Interoperability eXperiment (CWIX), which assesses federated Coalition capabilities within the NATO command construct via connected Live, Virtual, and Constructive (LVC) infrastructure. - Continue to develop and evaluate secure, interoperable technologies and capabilities supporting Denied, Degraded, Intermittent and Low-bandwidth (DDIL) operations including Allied/Coalition Shared Situational Awareness, cross-domain and data labeling solutions in maritime tactical networking environments, and advanced Information Assurance and Computer Network Defense (IA/CND) solutions (with common and interoperable processes and technologies). - Continue to evaluate technologies for interoperable maritime networking. Solutions will address higher bandwidth, Low Probability of Intercept (LPI)/Low Probability of Detection (LPD)/Anti-Jam (AJ) technologies across the Radio Frequency (RF) and Optical spectrum and include airborne capabilities. Evaluation of electromagnetic spectrum management and visualization technologies, force-level Electronic Warfare/Electromagnetic Maneuver Warfare (EW/EMW) will also enhance interoperable Information Warfare (IW). - Continue to enhance Allied IW interoperability leveraging joint and maritime multi-national forums, such as the Combined Communications Electronic Board (CCEB), Multinational Maritime Information-system Interoperability Steering Group (M2I2), and Mission Partner Environment/Future Mission Networking forums. - Continue to assess and validate individual technologies, integrated solutions, and associated Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) through experimentation, trials and demonstrations with Australia, Canada, New Zealand, United Kingdom, United States and other Allied/Coalition partners using Live, Virtual, Constructive, and Operational venues, such as the United States Navy (USN) Rim of the Pacific (RIMPAC), United Kingdom (UK) Joint Warrior events. - Continue evaluation of USN capabilities for conformance to NATO Federated Mission Networking Spiral Specification documentation. - Continue to evaluate existing/ emerging innovative technologies for value in increasing interoperability among US and Allied Nations, allowing them to act as force multipliers in Distributed Maritime Operations. - Continue to evaluate prospective technical capabilities and make recommendations to the Information Warfare acquisition community for integration of Allied Partner Nations into the Secret and Below Releasable Environment (SABRE).					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606355N / *Warfare Innovation Management*	**Project (Number/Name)** 0798 / *Allied/Coalition Maritime Environment (ACME)*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
- Utilize Combined Federated Battle Laboratories Network (CFBLNet) to baseline current expeditionary Mission Partner capabilities as they relate to interoperation with future enterprise Mission Partner Environment (Secret and Below Releasable Environment). - Leverage RIMPAC/Trident Warrior as well as other venues to demonstrate Threat Assessment, Blue Force Data Analysis, Tactical Data Movement, and effects Optimization is support of Australia/United Kingdom/United States (AUKUS) development efforts. ***FY 2025 Base Plans:*** - Continue to develop and evaluate secure, interoperable technologies and capabilities supporting Denied, Degraded, Intermittent and Low-bandwidth (DDIL) operations including Allied/Coalition Shared Situational Awareness, cross-domain and data labeling solutions in maritime tactical networking environments, and advanced Information Assurance and Computer Network Defense (IA/CND) solutions (with common and interoperable processes and technologies). - Continue to evaluate technologies for interoperable maritime networking. Solutions will address higher bandwidth, Low Probability of Intercept (LPI)/Low Probability of Detection (LPD)/Anti-Jam (AJ) technologies across the Radio Frequency (RF) spectrum. Evaluation of electromagnetic spectrum management and visualization technologies, force-level Electronic Warfare/Electro-magnetic Maneuver Warfare (EW/EMW) will also enhance interoperable Information Warfare (IW). - Continue to enhance Allied and Coalition Information Warfare interoperability with other joint and maritime multi-national forums, such as the Combined Communications Electronic Board (CCEB), Multinational Maritime Information-system Interoperability Steering Group (M2I2), Maritime Information Warfare Organization, and Mission Partner Environment/Future Mission Networking forums. - Continue to assess and validate individual technologies, integrated solutions, and associated Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) through experimentation, trials and demonstrations with Australia, Canada, New Zealand, United Kingdom, United States and other Allied/Coalition partners using Live, Virtual, Constructive, and Operational venues, such as the United States Navy (USN) Rim of the Pacific (RIMPAC), United Kingdom (UK) Joint Warrior events. - Continue use of a simulated NATO federated environment (Combined Federated Battle Laboratories Network) to demonstrate tactical operations in a future Mission Partner Environment via Coalition Warrior Interoperability eXperiment event. - Continue evaluation of USN capabilities for conformance to NATO Federated Mission Networking Spiral Specification documentation.					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606355N / *Warfare Innovation Management*	**Project (Number/Name)** 0798 / *Allied/Coalition Maritime Environment (ACME)*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
- Continue to evaluate existing/ emerging innovative technologies for value in increasing interoperability among US and Allied Nations, allowing them to act as force multipliers in Distributed Maritime Operations. - Continue to evaluate and make recommendations to the Information Warfare acquisition community for integration of Allied Partner Nations into the Secret and Below Releasable Environment (SABRE). -Continue leveraging the Combined Federated Battle Laboratories Network (CFBLNet) to assess Navy expeditionary Mission Partner capabilities as they relate to interoperation with future enterprise Mission Partner Environment (Secret and Below Releasable Environment). -Expand efforts to demonstrate Threat Assessment, Blue Force Data Analysis, Tactical Data Movement, and effects Optimization is support of Australia/United Kingdom/United States (AUKUS) development efforts. ***FY 2025 OCO Plans:*** N/A ***FY 2024 to FY 2025 Increase/Decrease Statement:*** No significant changes from FY24 to FY25.					
Accomplishments/Planned Programs Subtotals	1.229	7.317	7.189	0.000	7.189

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy			Date: March 2024
Appropriation/Budget Activity 1319 / 6	R-1 Program Element (Number/Name) PE 0606355N / *Warfare Innovation Management*	Project (Number/Name) 2144 / *Space & Elec Warfare Engineering*	

COST ($ in Millions)	Prior Years	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
2144: *Space & Elec Warfare Engineering*	0.000	26.729	15.167	28.698	-	28.698	29.605	30.061	30.663	31.281	Continuing	Continuing
Quantity of RDT&E Articles		-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

To support Navy objectives in advancing Information Warfare (IW) capabilities, the Space and Electronic Warfare (SEW) Engineering project provides three main functions:

(1) Navy Advanced Manufacturing (AdvM) technology aligns to Chief of Naval operations (CNO) priorities to deliver revolutionary capabilities to improve fleet readiness. These enterprise solutions will provide the foundation to (a) enhance warfighter capability by implementing disruptive AdvM technologies such as Additive Manufacturing (AM), Subtractive Manufacturing, 3D CNC milling, Computer Numerical Control (CNC) Lathing, and Robotic welding; (b) increase readiness through low-volume production of hard-to-source items; and (c) improve warfighting capacity by enabling low volume custom production at or near the point of need. Specific efforts include the development of the Digital Advanced Manufacturing Ecosystem (DAME) to address the design and certification of AM capabilities for both afloat and ashore, development of Cyber Security Risk Management Profiles for devices and applications on operational networks, definition of a secure Technical Data Package to describe components that can be digitally manufactured, and the development of an overarching, enterprise-level Digital Manufacturing Thread (device management, digital rights management, licensing, configuration management, data storage rule/access and application programming interfaces).

(2) Develop the architectures, specifications and standards, tools, and processes to support a single integrated Navy Cybersecurity plan. Develop cybersecurity engineering criteria within Navy specific guidance to drive common and consistent implementation of security controls within a threat informed mission impact approach across current and future Navy Programs of Record/projects. This eliminates redundancies and inefficiencies characteristic of previous stove-pipe development efforts in which each system addressed security individually. These efforts enable a standardized approach to improve the Navy's cyber resiliency to Cyber Adversary's weaponization of IT/OT susceptibility to attack. Provide the cybersecurity vulnerability and functional test standards, which supports cybersecurity test requirements and the Command, Control, Communications, Computers, Intelligence (C4I) components of Naval Information Warfare Systems Command (NAVWARSYSCOM) Information Warfare (IW) Kill Chain Testing for SYSCOM Red Team.

NAVWAR develops and deploys innovative Naval approach for rapid delivery of software applications with emphasis on security & automation via Certified Continuous Integration (CI) / Continuous Delivery (CD) pipeline tools based upon NAVWAR designed SECDEVOPS services under SECNAV Rapid Assess & Incorporate Software Engineering (RAISE). This combination of Systems Commands functions, services and tools ensures Navy platforms in operational maritime environments can effectively defend and "fight through" cyber adversary attacks under a framework of mission thread analysis and assessment.
NAVWAR establishes an integrated Enterprise Architecture to support design, development and delivery of integrated Navy Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), Business Information Technology (IT), and Space System capabilities. This architecture reflects current (as-is) and future (target) end states to support technical analyses, program planning, and enterprise-level investment decisions across IW capabilities on both ashore and afloat platforms. Provides engineering tools and processes to drive rigorous systems engineering discipline across the acquisition lifecycle to support rapid

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606355N / *Warfare Innovation Management*	**Project (Number/Name)** 2144 / *Space & Elec Warfare Engineering*

development and delivery of secure and interoperable C4ISR, Business IT, and Space Systems capabilities that meet Fleet requirements. Conduct Systems Engineering Technical Reviews (SETRs) to provide independent, objective assessments and certifications of technical maturity and compliance with applicable architectures, specifications and standards across IW capabilities.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Title: Advanced Manufacturing (AdvM)	2.559	3.118	2.925	0.000	2.925
Articles:	-	-	-	-	-
FY 2024 Plans: - Continue utilizing the Additive Manufacturing Test-Bed to further develop specifications, standards, and architecture/models to drive interoperability across the Navy / Joint Enterprise Digital Thread for Additive Manufacturing. - Continue to develop a systems engineering model to define the Additive Manufacturing Architecture that ties Logistics Information Technology (LOG IT) architecture and initial integration with the DoD Joint Additive Manufacturing Exchange (JAMEX) environment. - Deploy a product to the cloud environment to connect multiple Additive Manufacturing sites to a collaborative access point for 3D Models a from a shared repository through content management capability. - Continue development of the additive manufacturing data strategy. - Continue to define the Digital Manufacturing Strategy for integration into logistics Digital transformation plan.					
FY 2025 Base Plans: - Deployment and transition of technology and documentation associated with AM material recycling and filament creation technology. - Continue work on testing and validation of emerging AdvM tools and materials. - Continue cross-SYSCOM collaboration on AdvM training and sustainment of deployed equipment to facilitate distributed manufacturing capabilities. - Continue working across Navy system commands to reach the initial operational capability point for zero-trust and cloud-based cybersecurity solutions. - Continue onboarding customers in the Department of the Navy enterprise to the print tracking application to allow end-users to order, print, and track the part from point-of-manufacture to point-of-need. - Continue working across Navy systems commands to advance solutions for connecting repositories, data exchange, and exploring integration with external data sites. - Fully deploy the TDP application in the production cloud to streamline the automated development, process, and certification of AdvM Technical Data Packages for the Department of the Navy enterprise.					
FY 2025 OCO Plans:					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606355N / *Warfare Innovation Management*	**Project (Number/Name)** 2144 / *Space & Elec Warfare Engineering*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
N/A ***FY 2024 to FY 2025 Increase/Decrease Statement:*** No significant changes from FY24 to FY25.					
Title: System of Systems (SoS) Cybersecurity and Capability Engineering	13.068	6.659	25.773	0.000	25.773
Articles:	-	-	-	-	-
FY 2024 Plans: - Continue key efforts to develop technical architectures, tools, standards, and best practices to advance the Navy's integrated plan for effective implementation of resilient cybersecurity. These critical Cyber Security Technical Authority (CS TA) artifacts: (1) leverage CS TA Cyber Risk Assessments (CRA) to account for emerging cyber threats and advances in technology, (2) drive the use of Risk Management Framework (RMF) Rapid Assess and Incorporate (A&I) Software Engineering (RAISE) process for inheritance to reduce redundant cybersecurity investments, lower operational risk and significantly improve delivery times for emerging capabilities. - Continue to perform holistic Cyber Risk Assessments (CRA) that evaluate Navy systems in the context of warfighting missions across tabletop, lab, and operational environments. The results of the CS TA Tabletop Mission Cyber Risk Assessments (TMCRA), which examine access vectors and likelihood of adversary exploit, are tested in NAVWAR's IW Capability Testing environment, and are then used to support Navy-wide Live, Virtual, and Constructive (LVC) Information Warfare (IW) capability tests and Fleet experimentation. This holistic set of assessments allows Program Managers to include to mitigate existing risks across the system lifecycle as well as strengthen the cybersecurity design of future system variants. - Continue to develop automation of the RMF process, leveraging integrated digital engineering models that will streamline data and analytics to provide assessment results. The automated process includes integrating various RMF roles, data entry, and continued auditing/validating RMF steps (control selection, assessment, and authorization). Implement cyber operational risk threat assessments and continuous monitoring. ***FY 2025 Base Plans:*** - Continue key efforts to develop technical architectures, tools, standards, and best practices to advance the Navy's integrated plan for effective implementation of resilient cybersecurity. These critical Cyber Security Technical Authority (CS TA) artifacts: (1) leverage CS TA Cyber Risk Assessments (CRA) to account for emerging cyber threats and advances in technology, (2) drive the use of Risk Management Framework					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606355N / *Warfare Innovation Management*	**Project (Number/Name)** 2144 / *Space & Elec Warfare Engineering*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
(RMF) Rapid Assess and Incorporate (A&I) Software Engineering (RAISE) process for inheritance to reduce redundant cybersecurity investments, lower operational risk and significantly improve delivery times for emerging capabilities. - Continue to perform holistic Cyber Risk Assessments (CRA) that evaluate Navy systems in the context of warfighting missions across tabletop, lab, and operational environments. The results of the CS TA Tabletop Mission Cyber Risk Assessments (TMCRA), which examine access vectors and likelihood of adversary exploit, are tested in NAVWAR's IW Capability Testing environment, and are then used to support Navy-wide Live, Virtual, and Constructive (LVC) Information Warfare (IW) capability tests and Fleet experimentation. This holistic set of assessments allows Program Managers to include to mitigate existing risks across the system lifecycle as well as strengthen the cybersecurity design of future system variants. - Continue to develop automation of the RMF process, leveraging integrated digital engineering models that will streamline data and analytics to provide assessment results. The automated process includes integrating various RMF roles, data entry, and continued auditing/validating RMF steps (control selection, assessment, and authorization). Implement cyber operational risk threat assessments and continuous monitoring. Perform DON CISO Cyber Figure of Merit (CFOM) acquisition gate assessments, system of systems Cyber Risk to Mission (CRTM) assessments, develop and update cybersecurity technical standards, all of which support better understanding of and mitigation of cyber risk across the Navy. Advance the Continuous Monitoring (CONMON) and cyber operational picture capability required to meet Fleet Cyber Command (FCC) objectives. - Continue to perform Systems Engineering Technical Reviews (SETRs) across Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) and Digital Enterprise Services (DES); Manpower, Logistics, and Business Solutions (MLB) programs to ensure compliance with statutory and regulatory directives, as well as implementing applicable Information Technology (IT) and Cybersecurity (CS) Technology Authority (TA) architectures, specifications, standards, policies, processes and profiles. Continue efforts to integrate digital engineering advances as applicable to accelerate and automate SETR reviews to better support programs leveraging Agile or DevSecOps frameworks to support the Adaptive Acquisition Framework pathways. - Continue digital reviews for program certifications and technical reviews of formal acquisition and engineering documentation through enhanced design and testing analysis.					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606355N / *Warfare Innovation Management*	**Project (Number/Name)** 2144 / *Space & Elec Warfare Engineering*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
- Working to establish Enterprise Architecture to support design, development and delivery of integrated Navy Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), Business Information Technology (IT), and Space System capabilities. Perform mission-based system-of-systems kill chain and business thread analysis to ensure integration and interoperability, and validate end-to-end warfighting capabilities to address emerging threats. ***FY 2025 OCO Plans:*** N/A ***FY 2024 to FY 2025 Increase/Decrease Statement:*** Increase of $19.114M can be attributed to combining the SOS Capability Road Mapping and Engineering sub-project with this SoS Cybersecurity and Capability Engineering sub-project, as well as returning funding to prior year levels to support increased requirements for Enterprise Architecture, DON CISO Cyber Figure of Merit (CFOM) acquisition gate assessments, system of systems Cyber Risk to Mission (CRTM) assessments, Risk Management Framework (RMF) reform efforts to develop and advance the Continuous Monitoring (CONMON) and cyber operational picture capability required to meet Fleet Cyber Command (FCC) objectives. Increase also supports NAVWAR Digital Transformation efforts, system and system of systems model-based analysis, and the evolution of cybersecurity compliance activities.					
Title: System of Systems (SoS) Capability Roadmapping and Engineering	11.102	5.390	0.000	0.000	0.000
Articles:	-	-	-	-	-
FY 2024 Plans: - Continue to perform Systems Engineering Technical Reviews (SETRs) across Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) and Digital Enterprise Services (DES); Manpower, Logistics, and Business Solutions (MLB) programs to ensure compliance with statutory and regulatory directives, as well as implementing applicable Information Technology (IT) and Cybersecurity (CS) Technology Authority (TA) architectures, specifications, standards, policies, processes and profiles. Continue efforts to integrate digital engineering advances as applicable to accelerate and automate SETR reviews to better support programs leveraging Agile or DevSecOps frameworks to support the Adaptive Acquisition Framework pathways. - Continue digital reviews for program certifications and technical reviews of formal acquisition and engineering documentation through enhanced design and testing analysis. ***FY 2025 Base Plans:***					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606355N / *Warfare Innovation Management*	**Project (Number/Name)** 2144 / *Space & Elec Warfare Engineering*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
N/A ***FY 2025 OCO Plans:*** N/A ***FY 2024 to FY 2025 Increase/Decrease Statement:*** Decrease of $5.39M can be attributed to combining SoS Capability Roadmapping and Engineering subproject with the SoS Cybersecurity and Capability Engineering subproject beginning in FY 2025.					
Accomplishments/Planned Programs Subtotals	26.729	15.167	28.698	0.000	28.698

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy			Date: March 2024
Appropriation/Budget Activity 1319 / 6	R-1 Program Element (Number/Name) PE 0606355N / *Warfare Innovation Management*	Project (Number/Name) 3319 / *Fleet Experimentation*	

COST ($ in Millions)	Prior Years	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
3319: *Fleet Experimentation*	0.000	11.060	12.346	12.338	-	12.338	12.761	12.975	13.235	13.513	Continuing	Continuing
Quantity of RDT&E Articles		-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

Mission: The Fleet Experimentation (FLEX) program seeks out and examines potential materiel and non-materiel solutions and develops recommendations to enhance the Fleet's ability to execute assigned missions through conduct of 12 to 17 major analytic experimentation activities annually. The activities include workshops, war-games, with a focus on live force, operationally oriented at-sea events. The activities are integrated into a multi-year experiment campaign aligned to address selected Fleet priority capability gaps.

FLEX is co-led by Commander U.S. Fleet Forces Command (CUSFFC), Commander U.S. Pacific Fleet (CPF), and Commander U.S. Naval Forces Europe - Africa (CNE-AF). The three four-star Fleet Commanders identify the priority Fleet warfighting gaps that FLEX will address, and they drive refinements to FLEX planning, execution, and assessment/reporting processes.

Commanders' FLEX guidance is directly linked to the January 2022 Chief of Naval Operations (CNO) Navigation Plan (NAVPLAN) direction to continue refinement of concepts and capabilities through experimentation. FLEX priorities are aligned to CNO NAVPLAN Naval Integration Framework (NIF) pillars. FLEX planners collaborate directly with the NAVPLAN Integration Framework (NIF) teams to inform gap closure plans for Long Range Fires (Ca-5), Command and Control Counter-Intelligence, Surveillance, Reconnaissance, and Targeting (Ca-4), and Navy Operational Architecture (NOA) (Ca-2). Artificial Intelligence/Machine Learning (AI/ML) and Unmanned Systems, along with Naval Integration and Partner Nation integration, are considered enabling capabilities for FLEX. FLEX planners also collaborate with the AI NIF and Unmanned Task Force / Disruptive Capabilities Office.

FLEX initiatives are tied to CNO-approved Distributed Maritime Operations (DMO) concept capability requirements, Fleet warfighting gaps, and Key Operational Problems (KOP). FLEX aligns with National Defense Strategy priorities, lines of effort 1 (lethality) and 3 (reform), and numerous other strategic guidance documents highlighting the need to increase organizational learning and capability development in experimentation, wargames and exercises.

USFFC N8/N9-manages the FLEX investment -- $64.8M (FY25-FY29) - to support planning, execution, analysis, and reporting for analytically rigorous experiments leveraging small scale Limited Objective Experiments (LOE), scheduled fleet exercises, and high-end operational rehearsals such as Fleet Battle Problems (FBP) and Large Scale Exercises (LSE).

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Title: Fleet Experimentation (FLEX)	11.060	12.346	12.338	0.000	12.338
Articles:	-	-	-	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606355N / *Warfare Innovation Management*	**Project (Number/Name)** 3319 / *Fleet Experimentation*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Description: $12.3M in FY25 and $12.7M in FY26 will fund experimentation event planning, execution, analysis, and reporting to assess initiatives to implement Distributed Maritime Operations (DMO) and other Chief of Naval Operations (CNO) approved foundational warfighting concepts. Proposed experimentation initiatives and venues will be considered in early spring followed by formal approval in the summer. Tentative FLEX Campaign strategic areas are identified in the FY2025 Base Plans section of this document. Once approved, additional details can be provided on Secret Internet Protocol Router (SIPR) Network. Through experimentation, materiel and non-materiel solutions to concept required capabilities are tested and refined, and post-experiment recommendations support non-materiel solution implementation (e.g., TTP promulgation) and support NIF and program sponsor acquisition strategies, and inform procurement decisions. FLEX is a proven and efficient approach to improving warfighting effectiveness. FLEX deliverables are focused on operational and tactical warfighting capabilities in the near term (within the Future Years Defense Plan) and prioritized by annual FLEX Commanders' Guidance to enhance warfighting capability across priority warfare areas. FLEX venues and initiatives support the Chief of Naval Operations (CNO)-directed Fleet Battle Problems (FBP) and Large Scale exercises (LSE) series as identified in the DMO concept and the CNO Navigation Plan (NAVPLAN) signed in January 2022. ***FY 2024 Plans:*** FY24 and beyond FLEX efforts will address Fleet warfighting priorities. FLEX will continue to focus on materiel and non-materiel solutions using appropriate experimentation venues including workshops, wargames, and at-sea events. Alignment with IPLs, KOPs, DMO capability development and with NAVPLAN gap closure plans will drive experimentation efforts. The Fleet Commanders are expanding the warfighting gaps covered by the Commanders' FLEX Guidance to address capability shortfalls demonstrated in real world operations (details available on SIPRNET). Proposed initiatives have been coordinated with the Fleet Commanders' staffs and other stakeholders and are part of the FLEX Program's continuous approval process. Additional details about each experiment can be provided on SIPR. As of 3 Jan 2024					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606355N / *Warfare Innovation Management*	**Project (Number/Name)** 3319 / *Fleet Experimentation*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
FLEX in Integrated Battle Problem 23.3 ($404K) supports NOA, maritime fires, unmanned systems, Artificial Intelligence (AI)/Machine Language (ML), Allied/Partner Nation Integration, and Naval Integration FLEX in BOXER Amphibious Readiness Group (ARG) Marine Expeditionary Unit Exercise (MEUEX) ($556K) supports NOA, C5ISR, and Naval Integration TALISMAN TIG ($371K) supports maritime fires, unmanned systems, Artificial Intelligence (AI)/Machine Language (ML), and Naval Integration FLEX in Integrated Battle Problem 24.1 ($2.43M) supports NOA, C-C5ISRT, maritime fires, unmanned systems, Artificial Intelligence (AI)/Machine Language (ML), Allied/Partner Nation Integration, and Naval Integration Radiant United LOE ($356K) supportsC-C5ISRT Buzzer Beater LOE Phases 1 and 2 ($1.4M) supports maritime fires Northern Scissors TTX ($356K) supports C-C5ISRT FLEX in Valiant Shield 24 ($981K) supports NOA, C5ISR, C-C5ISRT, maritime fires, and Naval Integration FLEX in Baltic Operations (BALTOPS) 24 ($801K) supports NOA, C5ISR, unmanned systems, Artificial Intelligence (AI)/Machine Language (ML), and Allied/Partner Nation Integration FLEX in Integrated Battle Problem 24.2 ($2.45M) supports NOA, maritime fires, unmanned systems, Artificial Intelligence (AI)/Machine Language (ML), Allied/Partner Nation Integration, and Naval Integration FLEX LOE ($356K) supports C-C5ISRT BFTN Resilient Command and Control (RC2) System Enhancement (BRSE)RSE LOE ($646K) supports NOA, C5ISR, maritime fires, and Naval Integration FLEX in Atlantic Thunder 24 ($861K) supports NOA and C5ISR					
FY 2025 Base Plans: FY25 FLEX efforts will continue to address Fleet warfighting priorities identified in the Fleet Commanders' FLEX Guidance. Proposed capability solutions assessed in FLEX will focus on materiel and non-materiel solutions using appropriate experimentation venues including workshops, war-games, and at-sea events. Alignment with IPLs, KOPs, DMO capability development and with NAVPLAN gap closure plans will drive experimentation efforts. Initiatives will be collected, reviewed, and approved as part of the FLEX Program's continuous approval process. Tentative FLEX Campaign focus areas may include: Maritime Fires Counter-C5ISRT (C-C5ISRT) C5ISR					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606355N / *Warfare Innovation Management*	**Project (Number/Name)** 3319 / *Fleet Experimentation*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Naval Operational Architecture (NOA) Unmanned Systems (UxS) Artificial Intelligence / Machine Learning (AI/ML) Naval Integration (NI) Allied / Partner Nation Integration ***FY 2025 OCO Plans:*** N/A ***FY 2024 to FY 2025 Increase/Decrease Statement:*** No significant change from FY 2024 to FY 2025.					
Accomplishments/Planned Programs Subtotals	11.060	12.346	12.338	0.000	12.338

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy			Date: March 2024
Appropriation/Budget Activity 1319 / 6	R-1 Program Element (Number/Name) PE 0606355N / *Warfare Innovation Management*	Project (Number/Name) 3320 / *TRIDENT Warrior*	

COST ($ in Millions)	Prior Years	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
3320: *TRIDENT Warrior*	0.000	2.404	2.510	2.427	-	2.427	2.524	2.569	2.621	2.676	Continuing	Continuing
Quantity of RDT&E Articles		-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

U.S. Navy's Trident Warrior (TW) experiment campaign enables early delivery of Information Warfare (IW) capabilities to the warfighter via Fleet-directed TW operational events. It integrates stand-alone systems and efforts to achieve enhanced capabilities and demonstrates these capabilities in operational environments. This places innovative technologies into the hands of the warfighter to evaluate their effectiveness. Additionally, it develops supporting doctrine and Concepts of Operation to improve warfighting effectiveness. Coordinates IW efforts with other Service/Joint/Department of Defense/National efforts to ensure Joint/Interagency/ Allied/Coalition applicability and interoperability.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Title: Trident Warrior	2.404	2.510	2.427	0.000	2.427
Articles:	-	-	-	-	-
FY 2024 Plans: - Evaluate Trident Warrior 2023 (TW23) executed experiments and recommend next steps to all stakeholders. - Continue to promote broad participation in TW by researching advanced technology solution candidates, in conjunction with other services, and academic research in order to fill Information Warfare technology gaps. - In accordance with standardized procedures, lead TW participant efforts with the following: specific goal identification; risk identification; experiment plans (to include data requirements and collection); and required installation and security certifications, accreditations, and approvals. - Continue to provide independent experts and Subject Matter Expertise to ensure compliance with experiment plans, lead analysis effort, and deliver unbiased assessments and results to government sponsors to support the program's engineering recommendations. - Plan and execute Trident Warrior 2024 (TW24) with a continued focus on Information Warfare Operations and Overmatch related capabilities. - Begin Trident Warrior 2025 (TW25) planning, taking into consideration identified Naval Capability Gaps.					
FY 2025 Base Plans: - Evaluate Trident Warrior 2024 (TW24) executed experiments and recommend next steps to all stakeholders. - Continue to promote broad participation in TW by researching advanced technology solution candidates, in conjunction with other services, and academic research in order to fill Information Warfare technology gaps.					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606355N / *Warfare Innovation Management*	**Project (Number/Name)** 3320 / *TRIDENT Warrior*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
- In accordance with standardized procedures, continue to lead TW participant efforts with the following: specific goal identification; risk identification; experiment plans (to include data requirements and collection); and required installation and security certifications, accreditations, and approvals. - Continue to provide independent experts and Subject Matter Expertise to ensure compliance with experiment plans, lead analysis effort, and deliver unbiased assessments and results to government sponsors to support the program's engineering recommendations. - Plan and execute Trident Warrior 2025 (TW25) with a continued focus on Information Warfare Operations and Overmatch related capabilities. - Begin Trident Warrior 2026 (TW26) planning, taking into consideration identified Naval Capability Gaps. ***FY 2025 OCO Plans:*** N/A ***FY 2024 to FY 2025 Increase/Decrease Statement:*** No significant change from FY 2024 to FY 2025.					
Accomplishments/Planned Programs Subtotals	2.404	2.510	2.427	0.000	2.427

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A