Exhibit R-2, RDT&E Budget Item Justification: PB 2020 Navy											Date: March 2019	
Appropriation/Budget Activity 1319: *Research, Development, Test & Evaluation, Navy I* BA 6: *RDT&E Management Support*					R-1 Program Element (Number/Name) PE 0606942N *I (U)Assessments and Evals Cyber Vulnerabilities*							
COST ($ in Millions)	**Prior Years**	**FY 2018**	**FY 2019**	**FY 2020 Base**	**FY 2020 OCO**	**FY 2020 Total**	**FY 2021**	**FY 2022**	**FY 2023**	**FY 2024**	**Cost To Complete**	**Total Cost**
Total Program Element	0.000	0.000	48.800	0.000	-	0.000	0.000	2.000	2.000	2.000	Continuing	Continuing
4038: *Cyber Vulnerability Evaluation*	0.000	0.000	48.800	0.000	-	0.000	0.000	2.000	2.000	2.000	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Cyber Vulnerability Assessments and Evaluations program funds for cyber vulnerability assessments of major Navy weapons systems and cyber vulnerability assessments of critical shore infrastructure as directed by Sec. 1647 of the FY16 National Defense Authorization Act (NDAA) and Sec. 1650 of the FY17 NDAA, respectively. Funding will be used for assessments and non-recurring engineering for mitigations related to the Navy's major weapons systems identified in Joint Requirements Oversight Committee Memorandum (JROCM) 039-16 and on prioritized critical shore infrastructure prioritized.

Sec. 1647 of the FY16 NDAA directs the Secretary of Defense to complete an evaluation of the cyber vulnerabilities of each major weapon system of the Department of Defense by not later than December 31, 2019. Funded vulnerability assessments will build upon existing efforts regarding the identification and mitigation of cyber vulnerabilities of major weapons systems, and shall not duplicate similar ongoing efforts such as Task Force Cyber Awakening or conduct redundant assessment on systems that have already been evaluated.

Sec. 1647 assessment will be formalized in Vulnerability Assessment Reports (VARs), Cyber Table Top Exercises (CTTXs), Cyber Risk Analysis (CRAs) and other reporting.

Sec. 1650 of the FY17 NDAA directs the Secretary of Defense to submit a plan for assessing the cyber vulnerability of critical defense infrastructure and begin assessment of this infrastructure during a preliminary pilot program that will assess no fewer than two installations by December, 31 2019. Funded vulnerability assessments will end by calendar year 2020 and will build upon existing mission assurance, blue team, and red team capabilities. As instructed by the Congressional language, the assessments will utilize Department of Energy (DoE) and Department of Defense (DoD) national laboratory partnerships. Assessments will end with the submission of a final report to Congress. Strategies and procedures for mitigating the risk of cyber vulnerabilities should be identified during the course of evaluation.

Exhibit R-2, RDT&E Budget Item Justification: PB 2020 Navy	Date: March 2019
Appropriation/Budget Activity 1319: *Research, Development, Test & Evaluation, Navy I* BA 6: *RDT&E Management Support*	**R-1 Program Element (Number/Name)** PE 0606942N *I (U)Assessments and Evals Cyber Vulnerabilities*

B. Program Change Summary ($ in Millions)	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total
Previous President's Budget	0.000	48.800	0.000	-	0.000
Current President's Budget	0.000	48.800	0.000	-	0.000
Total Adjustments	0.000	0.000	0.000	0.000	0.000
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			

Change Summary Explanation

The funding decrease from FY 2019 to FY 2020 is due to the completion of the one year Cyber Vulnerability assessments of major Navy weapon systems and critical infrastructure.

Technical: Not applicable.
Schedule: Not applicable.

Exhibit R-2A, RDT&E Project Justification: PB 2020 Navy			Date: March 2019
Appropriation/Budget Activity 1319 / 6	R-1 Program Element (Number/Name) PE 0606942N / *(U)Assessments and Evals Cyber Vulnerabilities*	Project (Number/Name) 4038 / *Cyber Vulnerability Evaluation*	

COST ($ in Millions)	Prior Years	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
4038: *Cyber Vulnerability Evaluation*	0.000	0.000	48.800	0.000	-	0.000	0.000	2.000	2.000	2.000	Continuing	Continuing
Quantity of RDT&E Articles		-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The Cyber Vulnerability Assessments and Evaluations program funds for cyber vulnerability assessments of major Navy weapons systems and cyber vulnerability assessments of critical shore infrastructure as directed by Sec. 1647 of the FY16 National Defense Authorization Act (NDAA) and Sec. 1650 of the FY17 NDAA, respectively. Funding will be used for assessments and non-recurring engineering for mitigations related to the Navy's major weapons systems identified in Joint Requirements Oversight Committee Memorandum (JROCM) 039-16 and on prioritized critical shore infrastructure.

Sec. 1647 of the FY16 NDAA directs the Secretary of Defense to complete an evaluation of the cyber vulnerabilities of each major weapon system of the Department of Defense by not later than December 31, 2019. Funded vulnerability assessments will build upon existing efforts regarding the identification and mitigation of cyber vulnerabilities of major weapons systems, and shall not duplicate similar ongoing efforts such as Task Force Cyber Awakening or conduct redundant assessment on systems that have already been evaluated.

Sec. 1647 assessment will be formalized in Vulnerability Assessment Reports (VARs), Cyber Table Top Exercises (CTTXs), Cyber Risk Analysis (CRAs) and other reporting.

Sec. 1650 of the FY17 NDAA directs the Secretary of Defense to submit a plan for assessing the cyber vulnerability of critical defense infrastructure and begin assessment of this infrastructure during a preliminary pilot program that will assess no fewer than two installations by December, 31 2019. Funded vulnerability assessments will end by calendar year 2020 and will build upon existing mission assurance, blue team, and red team capabilities. As instructed by the Congressional language, the assessments will utilize DoE and DoD national laboratory partnerships. Assessments will end with the submission of a final report to Congress. Strategies and procedures for mitigating the risk of cyber vulnerabilities should be identified during the course of evaluation.
Program is to support Cyber Vulnerability Evaluations Assessments of E6B and Other Aviation Platforms.
The Cyber Vulnerability Assessments and Evaluations program funds for cyber vulnerability assessments of major Navy weapons systems and cyber vulnerability assessments of critical shore infrastructure as directed by Sec. 1647 of the FY16 National Defense Authorization Act (NDAA) and Sec. 1650 of the FY17 NDAA, respectively. Funding will be used for assessments and non-recurring engineering for mitigations related to the Navy's major weapons systems identified in Joint Requirements Oversight Committee Memorandum (JROCM) 039-16 and on prioritized critical shore infrastructure.

Sec. 1647 of the FY16 NDAA directs the Secretary of Defense to complete an evaluation of the cyber vulnerabilities of each major weapon system of the Department of Defense (DoD) by no later than December 31, 2019. Funded vulnerability assessments will build upon existing efforts regarding the identification and mitigation of cyber vulnerabilities of major weapons systems, and shall not duplicate similar ongoing efforts such as Task Force Cyber Awakening or conduct redundant assessment on systems that have already been evaluated.

Exhibit R-2A, RDT&E Project Justification: PB 2020 Navy		Date: March 2019
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606942N / *(U)Assessments and Evals Cyber Vulnerabilities*	**Project (Number/Name)** 4038 / *Cyber Vulnerability Evaluation*

Sec. 1647 assessment will be formalized in Vulnerability Assessment Reports (VARs), Cyber Table Top Exercises (CTTXs), Cyber Risk Analysis (CRAs) and other reporting.

Sec. 1650 of the FY17 NDAA directs the Secretary of Defense to submit a plan for assessing the cyber vulnerability of critical defense infrastructure and begin assessment of this infrastructure during a preliminary pilot program that will assess no fewer than two installations by December, 31 2019. Funded vulnerability assessments will end by calendar year 2020 and will build upon existing mission assurance, blue team, and red team capabilities. As instructed by the Congressional language, the assessments will utilize Department of Energy (DoE) and DoD national laboratory partnerships. Assessments will end with the submission of a final report to Congress. Strategies and procedures for mitigating the risk of cyber vulnerabilities should be identified during the course of evaluation.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total
Title: Cyber Vulnerability Evaluation for Ship Weapons Systems:	0.000	4.800	0.000	0.000	0.000
Articles:	-	-	-	-	-
FY 2019 Plans: CVN 78 - Analyze cybersecurity vulnerabilities using a system of systems approach and conduct system-of-systems cyber vulnerability assessments on CVN 78. - Utilize CVN 78 analysis to assess the vulnerability of the platform's vast control system networks. This assessment will play an integral role in identifying the most efficient and effective incremental improvements in CVN 78's cybersecurity, holistically maximizing cybersecurity of the platform's interconnected control system networks with the limited modernization budget available. -Execute modeling, simulation and analysis to capture system impacts of cyber vulnerabilities and identified mitigations, specifically situational awareness (SA) tools and continuous monitoring (CM) tools. - Leverage the model and analysis of CVN 78 as evidence of the platforms cyber survivability in a contested cybersecurity environment. The Cooperative Engagement Capability (CEC) and Navigation systems interface with multiple combat system and sensor types. Extensive and complex analysis is required to characterize and address cybersecurity and cyber vulnerability aspects of network operations over multiple interfaces. - Conduct a tabletop cyber assessment of critical hardware/software components and platform interfaces that could result in degradation of a mission enabling system. - Analyze cyber assessment results to determine the cyber resilience methods that could be further incorporated into modernization efforts.					

Exhibit R-2A, RDT&E Project Justification: PB 2020 Navy		Date: March 2019
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606942N / *(U)Assessments and Evals Cyber Vulnerabilities*	**Project (Number/Name)** 4038 / *Cyber Vulnerability Evaluation*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total
- Execute modeling, simulation and analysis to develop war fighting metrics to capture cyber vulnerabilities and identified mitigations to provide increased mission assurance. Ship Self Defense System (SSDS) -Conduct system-of-systems cyber vulnerability assessments on the SSDS Weapon System. - Identify elements within the Secure Combat System Domain, define threat scenarios, analyze risk through engineering assessments and table tops and prioritize development of cybersecurity capabilities to apply cyber controls and introduce resilience. - Ensure Combat System Enclave and networks successfully operate in adversarial cyber contested environment. ***FY 2020 Base Plans:*** N/A ***FY 2020 OCO Plans:*** N/A ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The decrease from FY 2019 to FY 2020 is due to the completion of the one year effort.					
Title: Cyber Vulnerability Assessments of Other Aviation Platforms	0.000	2.900	0.000	0.000	0.000
Articles:	-	-	-	-	-
FY 2019 Plans: - Conduct system-of-systems cyber vulnerability assessments on Other Aviation Platforms aircraft and associated support systems. - Execute modeling, simulation and analysis to capture the mission impacts of the cyber vulnerabilities. - Enhance emulation lab penetration testing capabilities to improve Other Aviation Platforms cyber risk assessment capacity and expand to include additional systems. - Conduct collaborative cyber security assessments and exercises with fleet operational community to assess vulnerability operational impacts and identify potential mitigations. - Align the cyber vulnerability assessments and findings to future Fleet or COCOM exercise(s). - Execute analysis and prototyping activities to mitigate identified cyber vulnerabilities. ***FY 2020 Base Plans:***					

Exhibit R-2A, RDT&E Project Justification: PB 2020 Navy		Date: March 2019
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606942N / *(U)Assessments and Evals Cyber Vulnerabilities*	**Project (Number/Name)** 4038 / *Cyber Vulnerability Evaluation*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total
N/A ***FY 2020 OCO Plans:*** N/A ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The decrease from FY 2019 to FY 2020 is due to the completion of the one year effort.					
Title: E6B ***Articles:*** ***FY 2019 Plans:*** - Conduct system-of-systems cyber vulnerability assessments on E-6B aircraft and associated support systems. - Execute modeling, simulation and analysis to capture the mission impacts of the cyber vulnerabilities. - Enhance emulation lab penetration testing capabilities to improve E-6B cyber risk assessment capacity and expand to include additional E-6B systems. - Conduct collaborative cyber security assessments and exercises with fleet operational community to assess vulnerability operational impacts and identify potential mitigations. - Align the cyber vulnerability assessments and findings to future Fleet or COCOM exercise(s). - Execute analysis and prototyping activities to mitigate identified cyber vulnerabilities. ***FY 2020 Base Plans:*** N/A ***FY 2020 OCO Plans:*** N/A ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The decrease from FY 2019 to FY 2020 is due to the completion of the one year effort.	0.000 -	2.100 -	0.000 -	0.000 -	0.000 -
Title: SWS Cyber Evaluations ***Articles:*** ***FY 2019 Plans:*** Conduct Trident system and sub-system cyber testing during Strategic Systems Programs (SSP) Development and Operational Testing. Conduct additional cyber testing to establish a cyber baseline for the current Strategic Weapon System. ***FY 2020 Base Plans:***	0.000 -	3.500 -	0.000 -	0.000 -	0.000 -

Exhibit R-2A, RDT&E Project Justification: PB 2020 Navy		Date: March 2019
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606942N / *(U)Assessments and Evals Cyber Vulnerabilities*	**Project (Number/Name)** 4038 / *Cyber Vulnerability Evaluation*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total
N/A ***FY 2020 OCO Plans:*** N/A ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The decrease from FY 2019 to FY 2020 is associated with the SWS Cyber Evaluations completing in FY 2019.					
Title: Trident System Cyber Hardening ***Articles:*** ***FY 2019 Plans:*** Conduct a tabletop cyber assessment of critical hardware/software components and platform interfaces that could result in a mission degrade. Analyze cyber assessment results to determine the cyber resilience methods that could be further incorporated into Strategic Weapon System modernization efforts. ***FY 2020 Base Plans:*** N/A ***FY 2020 OCO Plans:*** N/A ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The decrease from FY 2019 to FY 2020 is attributed to the Trident System Cyber Hardening completing in FY 2019.	0.000 -	5.500 -	0.000 -	0.000 -	0.000 -
Title: Cyber Vulnerability Assessments of Information Warfare Weapons Systems ***Articles:*** ***FY 2019 Plans:*** -Conduct system-of-systems cyber vulnerability assessments on Information Warfare Weapons Systems. -Execute modeling, simulation and analysis to develop warfighting metrics to capture the mission impacts of the cyber vulnerabilities and identified mitigations. -Overlay the cyber vulnerability assessment construct and findings during a major Fleet or Combatant Command (COCOM) exercise.	0.000 -	5.000 -	0.000 -	0.000 -	0.000 -

Exhibit R-2A, RDT&E Project Justification: PB 2020 Navy		Date: March 2019
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606942N / *(U)Assessments and Evals Cyber Vulnerabilities*	**Project (Number/Name)** 4038 / *Cyber Vulnerability Evaluation*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total
-Enhance red teaming and penetration testing capabilities to improve Navy cyber risk assessment capacity and proficiency. -Increase red teaming and penetration testing activities and conduct Navy Information Warfare cyber risk assessments. -Conduct cyber penetration testing to confirm/deny the presence of vulnerabilities and assess the effectiveness of mitigations. ***FY 2020 Base Plans:*** N/A ***FY 2020 OCO Plans:*** N/A ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The decrease from FY 2019 to FY 2020 is due to the completion of the one year effort.					
Title: Cyber Vulnerability Assessments of Critical Infrastructure	0.000	25.000	0.000	0.000	0.000
Articles:	-	-	-	-	-
Description: The Cyber Vulnerability Assessments and Evaluations program funds cyber vulnerability assessments of critical shore infrastructure as directed by Section 1650 of the FY17 National Defense Authorization Act (NDAA). Funding will be used for assessments of prioritized critical shore infrastructure. Sec. 1650 of the FY17 NDAA directs the Secretary of Defense to submit a plan for assessing the cyber vulnerability of critical defense infrastructure and begin assessment of this infrastructure during a preliminary pilot program that will assess no fewer than two installations by December, 31 2019. Funded vulnerability assessments will end by calendar year 2020 and will build upon existing mission assurance, blue team, and red team capabilities. As instructed by the Congressional language, the assessments will utilize DoE and DoD national laboratory partnerships. Assessments will end with the submission of a final report to Congress. Strategies and procedures for mitigating the risk of cyber vulnerabilities should be identified during the course of evaluation.					
FY 2019 Plans: Conduct comprehensive red (penetration-level), blue team assessments, and non-recurring engineering for mitigations identified related to facility related control systems. This includes those systems integrated into, as well as supporting, critical infrastructure for the Navy. As directed by Congressional language, these all-inclusive vulnerability assessments will require the development of multifaceted testing capabilities within the Navy shore domain while leveraging existing resources across the Fleet in addition to strategies and competencies					

Exhibit R-2A, RDT&E Project Justification: PB 2020 Navy		Date: March 2019
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0606942N / *(U)Assessments and Evals Cyber Vulnerabilities*	**Project (Number/Name)** 4038 / *Cyber Vulnerability Evaluation*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total
from our national laboratory partners. Supporting these vulnerability assessments will be the identification and development of mission modeling artifacts outlining the relationship between those identified facility related control systems and the relevant DoD and Navy mission and operational plans. These efforts will provide increased survivability and cyber resiliency of the Naval shore domain. ***FY 2020 Base Plans:*** N/A ***FY 2020 OCO Plans:*** N/A ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Funding decrease from FY 2019 to FY 2020 is due to the completion of assessments of cyber vulnerability of critical defense infrastructure as directed by Section 1650 of the FY17 National Defense Authorization Act (NDAA).					
Accomplishments/Planned Programs Subtotals	0.000	48.800	0.000	0.000	0.000

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

Deliverable of appropriate Cyber Vulnerability reports
Performance will be measured by Cyber Assessments completed.
Deliverable of appropriate Cyber Vulnerability reports.