

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Air Force **Date:** May 2021

Appropriation/Budget Activity 3600: <i>Research, Development, Test & Evaluation, Air Force I BA 7: Operational Systems Development</i>	R-1 Program Element (Number/Name) PE 0606942F / <i>Assessments and Evaluations Cyber Vulnerabilities</i>
--	--

COST (\$ in Millions)	Prior Years	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
Total Program Element	-	0.000	3.000	0.000	0.000	0.000	-	-	-	-	-	-
677821: <i>Cyberspace Vulnerability Assessment</i>	-	0.000	3.000	0.000	0.000	0.000	-	-	-	-	-	-
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-	-	-

A. Mission Description and Budget Item Justification

This program funds cyber vulnerability assessments of Air Force weapons systems and critical infrastructure as well as non-recurring engineering for mitigations. The effort leverages the methodology described in the Air Force Cyber Campaign Plan (CCP) to provide Air Force mission assurance in a cyber-contested environment. Under the Air Force CCP, the Air Force is accomplishing work mandated by Section 1647 of the Fiscal Year (FY) 2016 National Defense Authorization Act (NDAA) and Section 1650 of the FY 2017 NDAA. Section 1647 of the FY 2016 NDAA directs the Secretary of Defense to complete an evaluation of the cyber vulnerabilities of each major weapon system of the Department of Defense. Section 1650 of the FY 2017 NDAA mandates the Secretary of Defense submit a plan for assessing the cyber vulnerability of critical defense infrastructure and begin assessments of this infrastructure. This funding focuses on aspects of the Air Force CCP that develop processes, products, and people to perform the short term goals of conducting system cyber vulnerability assessments, cyber mitigations, and pilot programs and work toward the long term goal of achieving an enduring cyber resilient Air Force. The program builds upon existing efforts regarding the identification and mitigation of cyber vulnerabilities, and does not duplicate similar ongoing efforts or conduct redundant assessments on systems that have already been evaluated.

In addition, this program element may include necessary civilian pay expenses required to manage, execute, and deliver weapon system capability. It may also include necessary civilian pay expenses required to perform analysis and developmental activities required in support of the transition of weapon system capability. The use of such program funds would be in addition to the civilian pay expenses budgeted in program element 0605831F.

This program is in Budget Activity 7, Operational System Development because this budget activity includes development efforts to upgrade systems that have been fielded or have received approval for full rate production and anticipate production funding in the current or subsequent fiscal year.

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Air Force	Date: May 2021
--	-----------------------

Appropriation/Budget Activity 3600: <i>Research, Development, Test & Evaluation, Air Force I BA 7: Operational Systems Development</i>	R-1 Program Element (Number/Name) PE 0606942F / <i>Assessments and Evaluations Cyber Vulnerabilities</i>
--	--

B. Program Change Summary (\$ in Millions)	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
Previous President's Budget	0.000	0.000	0.000	0.000	0.000
Current President's Budget	0.000	3.000	0.000	0.000	0.000
Total Adjustments	0.000	3.000	0.000	0.000	0.000
• Congressional General Reductions	0.000	0.000			
• Congressional Directed Reductions	0.000	0.000			
• Congressional Rescissions	0.000	0.000			
• Congressional Adds	0.000	3.000			
• Congressional Directed Transfers	0.000	0.000			
• Reprogrammings	0.000	0.000			
• SBIR/STTR Transfer	0.000	0.000			
• Other Adjustments	0.000	0.000	0.000	0.000	0.000

Change Summary Explanation

FY 2021 increase of \$3.000 due to Congressional Add for Ransomware Response Exercise.

C. Accomplishments/Planned Programs (\$ in Millions)	FY 2020	FY 2021	FY 2022
<p>Title: Address Weapon System Cyber Vulnerabilities</p> <p>Description: Develop processes, products, and people to conduct weapon system cyber vulnerability assessments, cyber mitigations, demonstrations, and pilot programs toward the long term goal of achieving an enduring cyber resilient Air Force.</p> <p>FY 2021 Plans: Collaborate and coordinate with multiple Department of Defense organizations and Federal Government Agencies in developing and executing cybersecurity exercises related to ransomware response against weapon systems. These exercises will develop scenarios aimed at testing and developing concept of operations, courses of action, develop and apply TTPs while also documenting the aggressor's ransomware TTPs and methods impacting platform embedded systems. Identify and inform real-time cyber-defense operator training for ransomware attack response and corresponding mitigation efforts.</p> <p>FY 2022 Plans: Not Applicable</p> <p>FY 2021 to FY 2022 Increase/Decrease Statement: Effort Completion</p>	0.000	3.000	0.000
<p>Title: Address Infrastructure Cyber Vulnerabilities</p>	0.000	0.000	0.000

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Air Force		Date: May 2021		
Appropriation/Budget Activity 3600: <i>Research, Development, Test & Evaluation, Air Force I BA 7: Operational Systems Development</i>		R-1 Program Element (Number/Name) PE 0606942F / <i>Assessments and Evaluations Cyber Vulnerabilities</i>		
C. Accomplishments/Planned Programs (\$ in Millions)		FY 2020	FY 2021	FY 2022
<p>Description: Develop processes, products, and people to conduct infrastructure/control systems/Operational Technology cyber vulnerability assessments, cyber mitigations, demonstrations, and pilot programs toward the long term goal of achieving an enduring cyber resilient Air Force.</p> <p>FY 2021 Plans: Not Applicable</p> <p>FY 2022 Plans: Not Applicable.</p> <p>FY 2021 to FY 2022 Increase/Decrease Statement: Not Applicable.</p>				
<p>Title: Exercise Participation</p> <p>Description: This effort supports exercise participation, Combatant Command support, and assessment team activities to validate candidate weapon system and infrastructure cyber vulnerabilities.</p> <p>FY 2021 Plans: Not Applicable</p> <p>FY 2022 Plans: Not Applicable.</p> <p>FY 2021 to FY 2022 Increase/Decrease Statement: Not Applicable.</p>		0.000	0.000	0.000
Accomplishments/Planned Programs Subtotals		0.000	3.000	0.000
D. Other Program Funding Summary (\$ in Millions)				
N/A				
Remarks				
E. Acquisition Strategy				
When possible, activities in this effort will leverage current competitively-awarded contracts. Additional necessary contracts funded in this program element will be awarded using either competitive or sole source procedures, whichever is most appropriate. The government agency responsible for managing the program is the Air Force Life Cycle Management Center, Cyber Resiliency Office for Weapons Systems, Wright-Patterson Air Force Base, Ohio and Hanscom Air Force Base, Massachusetts.				

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Air Force **Date:** May 2021

Appropriation/Budget Activity 3600 / 7	R-1 Program Element (Number/Name) PE 0606942F / Assessments and Evaluations Cyber Vulnerabilities	Project (Number/Name) 677821 / Cyberspace Vulnerability Assessment
--	---	--

Product Development (\$ in Millions)				FY 2020		FY 2021		FY 2022 Base		FY 2022 OCO		FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract
Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost			
Industry Collaboration for Critical Infrastructure Mitigations (1650)	TBD	Various : TBD	-	0.000		-		-		-		-	-	-	-
More Situational Awareness for Industrial Control Systems (MOSAICS) SANDIA	MIPR	Albuquerque, NM : TBD	-	0.000		-		-		-		-	-	-	-
More Situational Awareness for Industrial Control Systems (MOSAICS)	MIPR	North Charleston, SC : TBD	-	0.000		-		-		-		-	-	-	-
Ransomware Response scenarios, courses of action, associated TTPs, and training requirements	Various	Various : TBD	-	-		3.000		-		-		-	-	-	-
Subtotal			-	0.000		3.000		-		-		-	-	-	N/A

Remarks
In FY 2019, the Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics transitioned the responsibility of funding NDAA 1647 and 1650 activities directly to the Services.

	Prior Years	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	0.000	3.000	-	-	-	-	-	N/A

Remarks
Ransomware response product development included in response to a FY 2021 Congressional Add

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Air Force		Date: May 2021
Appropriation/Budget Activity 3600 / 7	R-1 Program Element (Number/Name) PE 0606942F / <i>Assessments and Evaluations Cyber Vulnerabilities</i>	Project (Number/Name) 677821 / <i>Cyberspace Vulnerability Assessment</i>

	FY 2020				FY 2021				FY 2022				FY 2023				FY 2024				FY 2025				FY 2026							
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4				
<i>Cyberspace Vulnerability Assessment</i>																																
Conduct cyber vulnerability assessments for weapon systems	██████████																															
Develop and assess prototype weapon system cyber mitigations	██████████																															
Conduct Category 1 cyber vulnerability assessments for infrastructure	██																															
Conduct Category 2 cyber vulnerability assessments for infrastructure				██																												
Develop and assess infrastructure prototype cyber mitigations	██████████																															
Participate in exercises and red team activities	██████████																															
<i>Ransomware Response</i>																																
Identify and inform real-time cyber-defense operator training for responding to ransomware attacks					██████████																											
Develop ransomware scenarios aimed at testing and developing concept of operations, courses of action, develop and apply TTPs					██████████																											

UNCLASSIFIED

Exhibit R-4A, RDT&E Schedule Details: PB 2022 Air Force		Date: May 2021
Appropriation/Budget Activity 3600 / 7	R-1 Program Element (Number/Name) PE 0606942F / <i>Assessments and Evaluations Cyber Vulnerabilities</i>	Project (Number/Name) 677821 / <i>Cyberspace Vulnerability Assessment</i>

Schedule Details

Events by Sub Project	Start		End	
	Quarter	Year	Quarter	Year
<i>Cyberspace Vulnerability Assessment</i>				
Conduct cyber vulnerability assessments for weapon systems	1	2020	4	2020
Develop and assess prototype weapon system cyber mitigations	1	2020	4	2020
Conduct Category 1 cyber vulnerability assessments for infrastructure	2	2020	2	2020
Conduct Category 2 cyber vulnerability assessments for infrastructure	4	2020	4	2020
Develop and assess infrastructure prototype cyber mitigations	1	2020	4	2020
Participate in exercises and red team activities	1	2020	4	2020
<i>Ransomware Response</i>				
Identify and inform real-time cyber-defense operator training for responding to ransomware attacks	3	2021	4	2022
Develop ransomware scenarios aimed at testing and developing concept of operations, courses of action, develop and apply TTPs	3	2021	4	2022