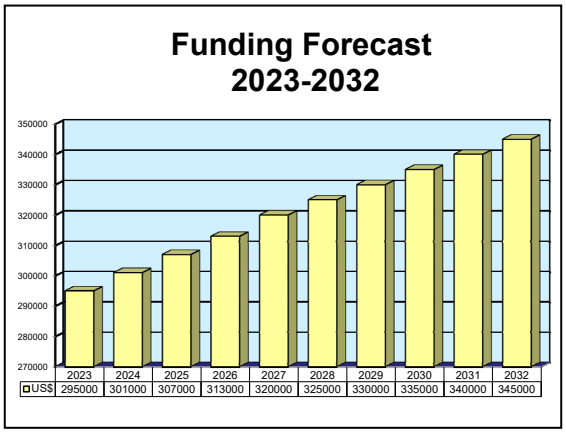
Cyber Defense Analysis

Outlook

- Stopping information leaks has become as important as stopping attacks
- Use of commercial, non-secure lines will increase due to overcrowding and a lack of available bandwidth space
- The focus of the program over the past few years has been on the development of data loss prevention technologies



Orientation

Description. The U.S. Air Force's Cyber Defense Analysis (CDA) weapon system project assesses non-secure telecommunications in order to determine the type and amount of sensitive and/or classified information that may have been disclosed to U.S. adversaries.

Status. Three units operational, with ongoing research and development.

Application. Cyber defense and cybersecurity.

Sponsor

U.S. Air Force
Air Combat Command
Joint Base Langley-Eustis, Virginia

Contractors

Contractor(s) not selected or not disclosed.

Contractors are invited to submit updated information to Editor, International Contractors, Forecast International, 75 Glen Road, Suite 302, Sandy Hook, CT 06482, USA; rich.pettibone@forecast1.com

Cyber Defense Analysis

Technical Data

The Cyber Defense Analysis (CDA) weapon system project is part of Program Element #0208088F AF Defensive Cyberspace Operations.

The CDA weapon system provides operational effects designed to protect and defend critical Air Force data at the nexus of adversarial threats and Air Force priorities and key missions. This weapon system evolved from operational security (OPSEC) programs designed to identify vulnerabilities for commanders in the field. The CDA project conducts operations in concert with Air Force Cyberspace Defense, Air Force Intranet Control, Cyberspace Vulnerability Assessment/Hunter, the Cyber Command and Control Mission System, and the Cyberspace Security Control System. The project conducts defensive cyberspace operations by monitoring, collecting, analyzing, and reporting on sensitive information released from friendly unclassified systems, such as computer networks, telephones, email, and Air Force websites. CDA is vital to identifying operations security disclosures and functions, and has a focus on data loss prevention and the conduct of information damage assessments.

CDA is operated by the 68th Network Warfare Squadron (active duty) at Joint Base San Antonio-Lackland, Texas, and by the 860th Network Warfare Flight and 960th NWF (Air Force Reserve) at Offutt Air Force Base, Nebraska.

CDA has two variants. Both are designed to monitor, collect, analyze and report on information transmitted via unsecure telecommunications systems to determine whether sensitive or classified information is being transmitted. Compromises are reported to field commanders, OPSEC monitors or others to determine potential impacts and operational adjustments. One of the variants, however, provides additional functionality to assess information damage based on network intrusions, and to assess unclassified Air Force websites. The second variant is only operated by the 68th NWS.

The CDA weapon system provides monitoring and/or assessment in six areas:

1. Telephony: Monitors and assesses unclassified Air Force voice networks.
2. Radio frequency: Monitors and assesses Air Force communications within the VHF, UHF, FM, HF and SHF frequency bands (mobile phones, land mobile radios, wireless local area networks).
3. Email: Monitors and assesses unclassified Air Force email traffic traversing the Air Force network.
4. Internet-based capabilities: Monitors and assesses information that originates within the AFNet that is posted to publicly accessible websites not owned, operated, or controlled by the Department of Defense or the federal government.
5. Cyberspace operational risk assessment: Assesses data compromised through AFNet intrusions with the objective of determining the associated impact on operations resulting from that data loss.
6. Web risk assessment: Assesses information posted on unclassified public and private websites that are owned, leased, or operated by the Air Force in order to minimize exploitation of Air Force information by potential adversaries.

Analyzing Cyberspace for Vulnerabilities

Source: U.S. Air Force

Program Review

Project Cyber Defense Analysis began in FY16. Details on recent activity follow.

The project schedule from FY16-FY20 called for supporting the technical maturation and development of CDA technologies to prevent the disclosure of sensitive and/or classified information to U.S. adversaries that attempt to penetrate networks.

The project schedule for FY21 called for continued support and development of data loss prevention technologies and insider threat detection capabilities. Additional support was given to the development of technology that blocks an adversary's attempts to get into U.S. networks.

AFINC Cyberspace Weapon System Attains Full Operational Capability

A major milestone was achieved on January 7, 2016 when the U.S. Air Force Intranet Control (AFINC) weapon system became the first cyberspace weapon system to reach Full Operational Capability (FOC). Achieving FOC means the AFINC system is fully capable of serving as the top-level defensive boundary and entry point for all network traffic into the Air Force Information Network (AFIN). The AFINC weapon system controls the flow of all external and inter-base traffic through standard, centrally managed gateways.

The AFINC weapon system consists of 16 Gateway suites, 15 SIPRNet nodes, 200+ service delivery points, and two Integrated Management suites, and is operated by the 26th Network Operations Squadron (26th NOS) located at Gunter Annex, Montgomery, Alabama.

The AFINC weapon system replaced and consolidated 100+ regionally managed disparate Air Force network entry points into 16 centrally managed access points for all traffic through the Air Force network. The AFINC weapon system provides greater agility to take defensive actions across the network. AFINC was officially designated a weapon system by the Air Force Chief of Staff in March 2013 and achieved Initial Operational Capability (IOC) in May 2014.

The AFINC Cyberspace Weapon System serves more than one million Air Force users at 237 sites worldwide. This infrastructure is among the largest in the world, yet is operated and maintained by a single Air Force unit. Over time the weapon system and 26th NOS operations have evolved to the point that the mission set now includes intelligence gathering, cyberspace surveillance and reconnaissance, interdiction, and security operations.

As mentioned in **Tactical Data**, other cyberspace weapons systems include the Air Force Cyberspace Defense weapon system, the Air Force Intranet Control weapon system, the Cyber Command and Control Mission System weapon system, the Cyberspace Defense weapon system, and the Cyberspace Vulnerability Assessment/Hunter weapon system.

Second Cyberspace Weapon System Reaches FOC

U.S. Air Force Space Command achieved a significant milestone on February 12, 2016, when the Cyberspace Vulnerability Assessment/Hunter weapon system reached FOC. The CVA/H weapon system enables the execution of vulnerability assessments, adversary threat detection, and compliance evaluations. CVA/H is a tool for cyber defense used inside the boundaries of the defended cyber system. The Air Force equips its Cyber Protection Teams with the CVA/H weapon system. The system provides the ability to find, track, target, engage and assess advanced persistent threats to AF missions on prioritized network enclaves within the AFIN.

CVA/H operators focus on providing vulnerability assessment and the Hunter mission. The Hunter mission provides the 24th Air Force commander and supported combatant commanders with a deployable, precision capability to identify, pursue within network boundaries, and mitigate cyberspace threats impacting critical links and nodes in support of theater or functional operations. The CVA/H weapon system provides in-depth assessment of information system assets such as computers, infrastructure, applications, data, and cyberspace operations.

The CVA/H weapon system consists of four primary components: the Mobile Interceptor Platform, the Deployable Interceptor Platform, the Garrison Interceptor Platform, and the Information Operations Platform-Fly Away Kit.

Active-duty weapon system operations are conducted by the 92nd Cyberspace Operations Squadron and the 834th Cyberspace Operations Squadron, located at Joint Base San Antonio-Lackland, Texas; and the 835th COS and 837th COS, located at Scott Air Force Base, Illinois. The Air Force Reserve Command is building a "classic associate" unit at Scott AFB to employ the CVA/H. Also, 12 Air National Guard units employ the weapon system. The system requires four operators, one cyberspace operations controller, and three cyberspace defense analysts.

Cyber Defense Analysis

CVA/H was officially designated a weapon system by the Air Force Chief of Staff in March 2013 and achieved IOC in June 2013.

"Weapon system" is a term used to identify requirements and critical resources to ensure that they receive comprehensive and equitable consideration for program-associated funding. It does not mean that the particular resource is a weapon as defined by the Air Force and Department of Defense.

Funding

U.S. FUNDING

	FY21 AMT	FY22 AMT	FY23 AMT	FY24 AMT	FY25 AMT	FY26 AMT	FY27 AMT	FY28 AMT
RDT&E (U.S. Air Force)								
PE#0208088F AF Defensive Cyberspace Operations: Project 822 Cyber Defense Analysis	0.279	0.281	0.295	0.301	0.307	0.313	0.320	N/A

All $ are in millions.

N/A = Not Available

Source: U.S. Air Force FY21 RDT&E Budget Document

Contracts/Orders & Options

No contracts valued over $5 million have been identified for this effort.

Worldwide Distribution/Inventories

The **U.S. Air Force** sponsors the Cyber Defense Analysis project.

Forecast Rationale

Overseen by the U.S. Air Force, the Cyberspace Defense Analysis (CDA) weapon system conducts Defensive Cyberspace Operations (DCO) and network defense by monitoring, collecting, analyzing, and reporting on sensitive information transiting or residing on the AFNet. CDA is the cyberspace weapon system used to conduct assessments during peacetime and contingency operations. Without proper funding, CDA operators will not be able to determine the potential damage and impact resulting from network intrusions. Operators will additionally not be able to determine the operational adjustments needed to maintain the system.

Despite the program being considered vital in a day and age where cyberspace protection is more important than ever, funding is expected to remain low over the forecast period – roughly, under half a million dollars a year. However, while low, it will remain stable and likely increase in the outer years, reflecting the importance of the system's role in national defense. The growing need for cybersecurity is sure to bring the program more attention in the coming years.

Ten-Year Outlook

ESTIMATED CALENDAR YEAR RDT&E FUNDING (in US$)												
Designation or Program		High Confidence				Good Confidence			Speculative			
	Thru 2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	Total
MFR Varies												
Cyber Defense Analysis												
	1,868,000	295000	301000	307000	313000	320000	325000	330000	335000	340000	345000	3,211,000
Total	1,868,000	295000	301000	307000	313000	320000	325000	330000	335000	340000	345000	3,211,000