DoD (//www.fifthdomain.com/dod/)

Here’s how DoD will invest in the cyber mission

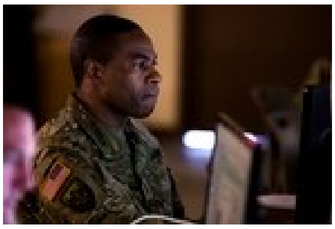
Insights into specific military cyber programs can be challenging. However, recently available budget documents provide a peek into how the Department of Defense seeks to equip and train cyberwarriors.

Specifically, details regarding U.S. Cyber Command’s two most well know, and largely funded, programs — Unified Platform and the Persistent Cyber Training Environment — are clearer.

Unified Platform

In the past, the services developed their own disparate platforms for operations. Given the joint nature of cyberspace operations, DoD decided it needed a singular platform — as well as tools — that the entire cyber mission force will use. The command established something called the Joint Cyber Warfighting Architecture (https://www.fifthdomain.com/dod/cybercom/2019/02/19/cyber-commands-2019-plan-for-new-tools/) to guide capability development priorities across the services for singular joint use.

Unified Platform will provide the cyber mission force an infrastructure capable of mission planning, data analytics and decision support, according to Air Force budget documents released March 18. The Air Force is procuring the system on behalf of Cyber Command and the joint force.



(https://www.fifthdomain.com/dod/2019/01/10/dod-ramps-up-development-of-a-cyber-factory/)

DoD ramps up development of a ‘cyber factory’ (https://www.fifthdomain.com/dod/2019/01/10/dod-ramps-up-development-of-a-cyber-factory/)

The Department of Defense is rapidly working to provide cyberwarriors capabilities under the Unified Platform.

By: Mark Pomerleau

“Unified Platform provides the Cyber Mission Forces … a Joint cyber operations infrastructure enabling full spectrum cyberspace operations at the operational through tactical levels of warfare. The DoD, AF, and the Cyber Mission Force require an interconnected and interoperable cyber infrastructure to conduct integrated planning and execution of cyberspace operations,” the documents state.

“Unified Platform delivers this capability through the integration of disparate, service-specific platforms and systems, infrastructure, mission capabilities, data analytics, and programs to build interoperable and scalable network for cyber capabilities.”

The recently released budget documents paint a better picture of investments and direction for Unified Platform.

(https://www.fifthdomain.com/dod/cybercom/2019/02/19/cyber-commands-2019-plan-for-new-tools/)

Cyber Command’s 2019 plan for new tools (https://www.fifthdomain.com/dod/cybercom/2019/02/19/cyber-commands-2019-plan-for-new-tools/)

Cyber Command is moving out on several fronts to begin developing its own infrastructure and tools for cyber warriors.

By: Mark Pomerleau

The documents note that FY20 funds requested will procure hardware for the effective deployment of operational capability to the cyber mission force.

In the base procurement budget, the Air Force is asking for $4.9 million. However, research and development requests reveal a much more hefty spend.

Under two separate elements, the Air Force is asking for a total of $10 million split evenly between “AF Prototyping” and “USCYBERCOM Prototyping” program elements.

Efforts under Air Force prototyping include initially developing the minimum viable product baseline from existing best of breed systems. FY20 plans include development of incremental operational capability addressing highest priority user requirements. The document states that funding decreased from last year to this year under this effort due to integration of Air Force prototyping efforts into Unified Platform baseline and a reduction of rapid prototyping activity.

Efforts under Cyber Command prototyping include supporting prototyping efforts associated with the research, development and integration of cyber technologies supporting the Unified Platform program. There was also a decrease in funding from last year to this year with the same reasons listed above.

Additionally, the Air Force is asking for $84.7 million under another portion of the research and development budget. This request, called “Foundational Efforts,” seeks to ensure perpetual capability development, integration and delivery of Unified Platform capability through an agile development process. Funding for this item increased by roughly $55 million from last year to this year due to additional war-fighter capability requirements required of the Unified Platform baseline, the document said.

The document also notes that after Unified Platform delivers a minimum viable product, which officials have said could be available as soon as this spring, subsequent build iterations will continue to deliver enhanced capabilities.

(https://www.fifthdomain.com/dod/cybercom/2018/12/06/tools-from-cyber-carrier-could-be-available-this-spring/)

Tools from ‘cyber carrier’ could be available this spring (https://www.fifthdomain.com/dod/cybercom/2018/12/06/tools-from-cyber-carrier-could-be-available-this-spring/)

The Unified Platform team is expected to deliver a minimal viable product in the spring.

By: Mark Pomerleau

The current approach seeks to leverage a rapid prototyping effort to deliver a set of capabilities over time through a variety of contracts.

Northrop Grumman was previously awarded a $54 million contract (https://www.fifthdomain.com/dod/cybercom/2018/10/29/cyber-command-awards-54m-contract-for-cyber-carrier/) to be the system coordinator. Additional awards include one for cyber enterprise services, which will enhance cyber platforms, as well as several others to include individual tools.

The documents note a variety of contract vehicles the Air Force will use for Unified Platform, to include Government-Wide Acquisition Contract (GWAC) vehicles (Alliant, Encore II, Solutions for Enterprise-Wide Procurement IV (SEWP IV), and General Services Administration (GSA) Federal Supply Schedules and a new Cyber Indefinite Delivery Indefinite Quantity (IDIQ) contract. The documents also indicate that the program envisions multiple-award contract vehicles, which will provide “a wide range of commercially-available products and services that can meet many requirements related to Unified Platform.”

Budget documents also point to timelines for potential awards on other elements of the program. They include:

- Agile capability development – October 2019

- Distributed common development/integration environment – February 2020
- Distributed common staging environment – February 2020

Persistent Cyber Training Environment (PCTE)

Cyber forces currently lack a robust training environment similar to what forces in the physical world enjoy for either individual or collective training. A common parallel in the physical world are the Army's combat training centers.

PCTE will fill this void allowing for individual and collective training, as well as mission rehearsal.

(https://www.fifthdomain.com/dod/2018/10/25/cyber-operators-get-first-crack-at-training-platform/)

Cyber operators get first crack at training platform (https://www.fifthdomain.com/dod/2018/10/25/cyber-operators-get-first-crack-at-training-platform/)

The Army recently concluded the first user assessment for the Persistent Cyber Training Environment.

By: Mark Pomerleau

Currently, the Army is running a series of innovation challenges leveraging small companies to prototype the effort in order to inform the larger program more holistically. While the government is currently operating as the system integrator, the plan is to eventually hand that role off to a contractor.

Funded by the Army on behalf of Cyber Command and the joint force, Army budget documents note base procurement funding for PCTE in FY20 for $3 million. This will provide hardware and operations systems required to expand PCTE services from the regional compute and storage node to the training facility. Additionally, it will provide hardware end points at the training facility.

Procurement funding will support the migration of PCTE to DoD enterprise networks, as well as government and/or commercial cloud environments.

Army research and development budget documents request $52.1 million for PCTE, which span across several individual projects. Army research and development documents from last year indicate it planned to spend $65.1 million in FY20 for this same effort.

(https://www.fifthdomain.com/dod/2018/02/21/army-requests-429-million-for-new-cyber-training-platform/)

Army requests $429 million for new cyber training platform (https://www.fifthdomain.com/dod/2018/02/21/army-requests-429-million-for-new-cyber-training-platform/)

Army budget documents outline how much the service is looking to spend on one of its top priorities: the Persistent Cyber Training Environment.

By: Mark Pomerleau

The various projects include:

- Event management ($25.6 million) — Develop event scheduling, allocation and management function for PCTE to include design, planning and execution supported. FY20 plans include expansion of fielded PCTE capabilities to include automated opposition force.
- Environment operations and management ($13.4 million) — Develop PCTE with realistic vignettes and scenarios as part of a syllabus of individual and collective training to include real-world mission rehearsal. FY20 plans include continuing to build and host virtual environments of actual network systems to include industrial control systems, supervisory control and data acquisition systems.
- Physical and virtual connectivity ($10.6 million) — On-demand reliable, secure and physical and virtual global access to the system. FY20 plans include extending connectivity to more regional base training facilities to include National Guard and Reserve cyber mission force teams.
- Test and evaluation ($2.5 million) — Integration, development and operational testing. FY20 plans note that testing is essential this year to ensure any fielded capability drop does not break existing PCTE platform and training capabilities.

Recommended for you

Meet the scholar challenging the cyber deterrence paradigm

The Army’s next question: should battlefield commanders have cyber capabilities?

(http://www.fifthdomain.com/home/2017/07/19/meet-the-scholar-challenging-the-cyber-deterrence-paradigm/?utm_source=clavis)

Estonian official: Cyber must be part of core military education

(http://www.fifthdomain.com/2017/11/21/estonian-official-cyber-must-be-part-of-core-military-education/?utm_source=clavis)

(http://www.fifthdomain.com/dod/army/2018/03/13/th
armys-next-question-should-battlefield-commanders-have-cyber-capabilities/?utm_source=clavis)

Among Pentagon's New Year's resolutions: more cyber

(http://www.fifthdomain.com/dod/2018/01/02/among-
pentagons-new-years-resolutions-more-cyber/?utm_source=clavis)

Around the Web

Comments

Most Watched Videos

▶ Play

How the shutdown is affecting federal cybersecurity (/video/2019/01/14/how-the-shutdown-is-affecting-federal-cybersecurity/)

Fifth Domain speaks with Darien Kindlund, of Insight Engines on the 21st day of the federal government shutdown. (Daniel Woolfolk/Staff) (/video/2019/01/14/how-the-shutdown-is-affecting-federal-cybersecurity/)

How to stay anonymous for feds (Part 2)

▶ Play Video

(/video/2018/11/16/how-to-stay-anonymous-for-feds-part-2/)

Estonia wants to shape world cyber laws on UN Security Council

▶ Play Video

(/video/2018/11/12/estonia-wants-to-shape-world-cyber-laws-on-un-security-council/)

A key factor to Estonia's cyber success (which the US has yet to replicate)

▶ Play Video

(/video/2018/11/05/a-key-factor-to-estonias-cyber-success-which-the-us-has-yet-to-replicate/)

Top Headlines (//www..com/)

✉ Newsletters (https://link.fifthdomain.com/join/5ft/sign-up)
Contact Us (/contact-us)

Civilian (/civilian) **DoD (/dod)** **Congress (/congress)**
Critical Infrastructure (/critical-infrastructure) **International (/international)**
Workforce (/workforce) **Industry (/industry)** **Thought Leadership (/thought-leadership)**

Terms of Use
Terms of Service (http://sightlinemediagroup.com/terms-of-service/)
Privacy Policy (/privacy)
()
()

Get Us
Newsletters & Alerts (https://link.fifthdomain.com/join/5ft/sign-up)

RSS Feed (/rss)
()
()

Contact Us

Help & Contact Info (/contact-us)
Advertise (/advertising)
()
()

About Us

About Us (/about-us)
Careers (https://boards.greenhouse.io/sightlinemediagroup?gh_src=cpxe2a1)
()
()

Military News (https://www.militarytimes.com) Air Force News (https://www.airforcetimes.com)

Army News (https://www.armytimes.com)

Marine Corps News (https://www.marinecorpstimes.com)

Navy News (https://www.navytimes.com) Defense News (http://www.defensenews.com)

Federal News (http://www.federaltimes.com) C4ISR (http://www.c4isrnet.com)

Cyber (http://www.fifthdomain.com/) History (http://www.historynet.com/)