

780th MILITARY INTELLIGENCE BRIGADE (CYBER)

THE BYTE

Vol. 14, Issue 3

July 2026



THIS WE'LL DEFEND:
Delivering Ready Combat Formations



251st
ARMY
BIRTHDAY





780th MI BDE
"STRENGTH AND HONOR"

COL Candy Boparai
Commander
CSM Joseph Daniel
Command Sergeant Major

780th MILITARY INTELLIGENCE BRIGADE (CYBER), Fort George G. Meade, Maryland, publishes The BYTE as an official command information publication, authorized under the provisions of AR 360-1, to serve its Soldiers, Civilians, and Families.

Opinions expressed herein do not necessarily represent those of 780th MI BDE or the Department of the Army.

All photographs published in The BYTE were taken by 780th MI BDE Soldiers, Army Civilians, or their Family members, unless otherwise stated.

Send articles, story ideas, photographs, and inquiries to the 780th MI Brigade (Cyber) Public Affairs Officer (PAO) and The BYTE Editor, Steven Stover at steven.p.stover.civ@army.mil, or mail to 310 Chamberlin Avenue, Fort George G. Meade, MD 20755, or call (301) 833-6430.



Always in the Fight: Reflections from the Eighth Praetorian Brigade Commander
COL Candy Boparai, CDR, 780th MI BDE (Cyber)

Operations Support Change of Command Ceremony

780th MI BDE (Cyber) PAO

781st Military Intelligence Battalion (Cyber), Vanguard Change of Command Ceremony

780th MI BDE (Cyber) PAO

The Joint Command and Control and Mission Command

CPT Brendan Vito Stonionis, 781st MI BN (Cyber)

Beyond the Checkbox:

Lessons from FMQ and What Proficiency Fit Must Get Right

CPT Daniel Alvarado, 781st MI BN (Cyber)

A Unified Front: How the 780th MI BDE Delivers Holistic Cyber Readiness

SGT Jaysen Johnson, DET-TX, 782d MI BN (Cyber)

The Revised Cyber Force Generation Model: A Framework for Operational Readiness

CW2 Melanie Wahl and Mr. Mike Holdway, D Co., 782d MI BN (Cyber)

Army Cyber Capability Developers and Cyber Warfare Battalion Collaborate on Drone Dominance

SPC William Perez, CSD-Maryland, OSE

Preparing Cyber Formations for Tactical Operations

CPT Curtis Peters, A Co., 11th CWB

The Road to Drone Dominance:

Drones without the Dollars

1LT Omkar Kale, B Co., 11th CWB

Praetorian Brigade Command Chief Warrant Officer James Richards Retires after 24 Years of Army Service

780th MI BDE (Cyber) PAO

HHC (Hastati), 780th MI Brigade (Cyber) Change of Command Ceremony

1

3

5

7

8

11

13

15

17

20

23

27

CISA Announces Winners of the 2026 President’s Cup Cybersecurity Competition	29
A Final Honor: <i>Inside the Fort Meade Military Funeral Honors Mission</i> Ms. Abigail Carey, FGGM Public Affairs	31
Honoring Our Fallen “Lest We Forget”	33
Praetorian Soldiers Represent Army Cyber Bataan Memorial Death March	35
Fort Meade Spring Fest	36
Sharing How the Next Generation Can Be All They Can Be	37
NCOPD PT Session	38
Joint Language Wars 2026	39





Always in the Fight: *Reflections from the Eighth Praetorian Brigade Commander*

By COL Candy Boparai, Commander, 780th Military Intelligence Brigade (Cyber)

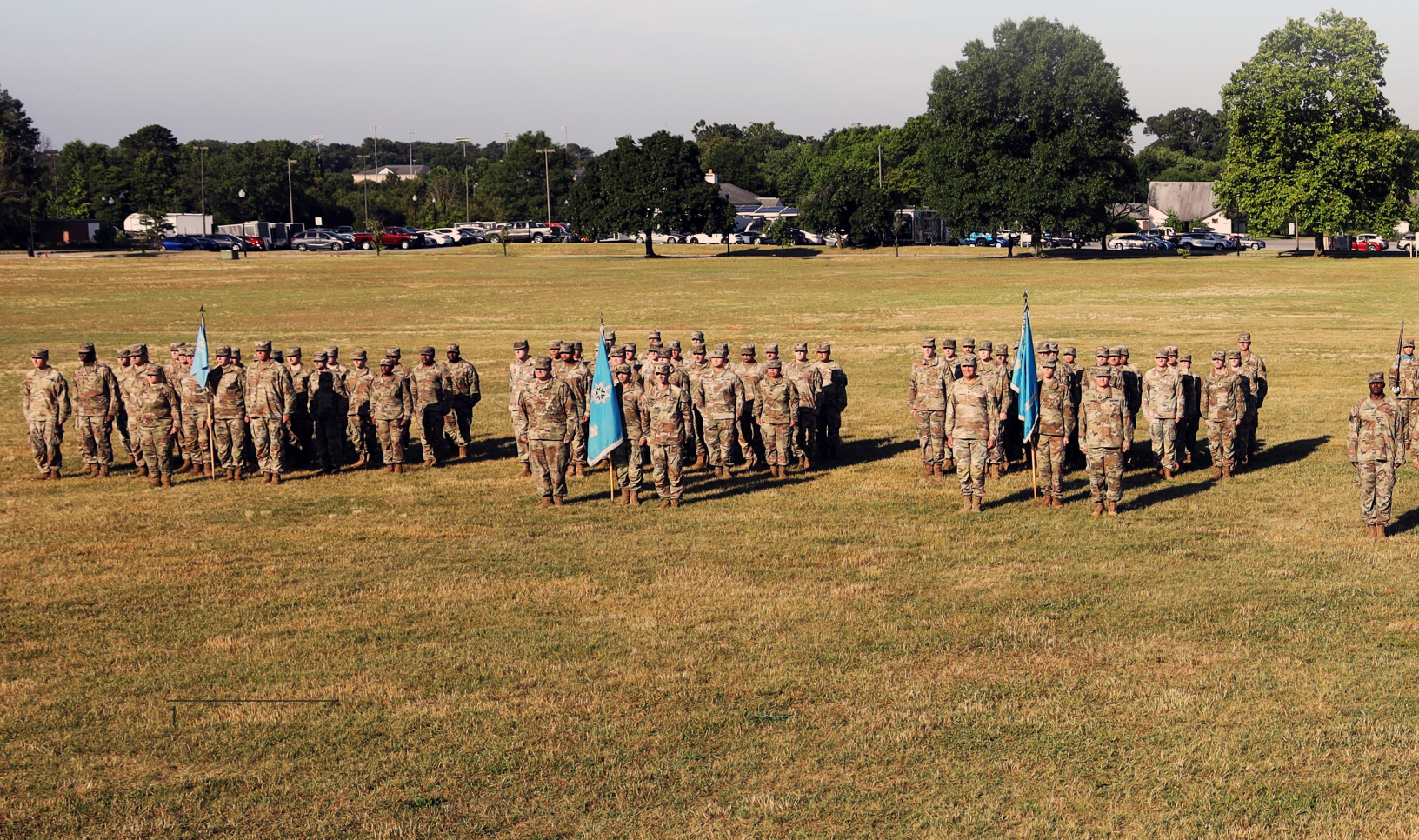
WHEN I ASSUMED COMMAND OF THE 780TH MILITARY INTELLIGENCE BRIGADE (CYBER), as a Brigade alum I knew that I was stepping into an organization unlike any other in the United States Army. As the Army's sole offensive cyberspace operations brigade, we enable operations at the cutting edge of national security, executing missions that are often unseen but profoundly impactful.

As I prepare to relinquish command this month, I want to take this opportunity to reflect on what we—the Soldiers, Civilians, and Families of the Praetorian Brigade—have accomplished together.

Over the past two years, the operational environment has evolved at a blistering pace. Our adversaries have grown more sophisticated, and the demand for our unique capabilities has never been higher. Yet, time and again, this brigade has met those challenges head-on. From Fort George G. Meade to Fort Gordon, and across our detachments in Texas and Hawaii, you have consistently delivered decisive effects for Army Cyber Command and the Joint Force.

What I am most proud of, however, is not just what we have accomplished, but how we have accomplished it.

We prioritized “People First” not as a slogan, but as an operational necessity. We



championed the Work Role Certification Incentive Program, ensuring our technical experts were recognized and rewarded for mastering their craft. We strengthened our training pipelines, emerged after iterative Civilian workforce changes, rapidly pivoted combat power in support of emerging missions, and strengthened a command climate built on mutual respect and unrelenting professionalism.

To the “Hastati” of the Brigade HHC, the “Vanguard” of the 781st, the “Cyber Legion” of the 782d, the “Leviathans” of the 11th Cyber Warfare Battalion, and our OSE Developers: your dedication to the mission is awe-inspiring. You have set the standard for what a modern, technically elite fighting force looks like.

To the Families who support our Service Members and Civilians: your sacrifices make our operations possible. Thank you for your unwavering resilience.

As I transition command to COL Ben Klimkowski, I do so with the utmost

confidence in the future of this brigade. I have known COL Klimkowski for years – he is an exceptional leader who deeply understands this mission and this workforce. He is tailor-made for the Brigade we are now. I know you will support him and his family with the same dedication, excellence, and care as you have shown me and my family.

As I approach change of command, I feel a sense of deep gratitude. Gratitude to the multitude of people who have helped me and the Brigade, and particularly, gratitude to all of you for everything you do every day for the mission, and for each other. Serving as your commander has been the greatest honor of my career. The work you do is vital to the defense of our nation. Continue to push the boundaries, take care of one another, and uphold the Praetorian standard.

Everywhere and Always....in the Fight! ■





Operations Support Element Change of Command Ceremony

By the 780th Military Intelligence Brigade (Cyber) Public Affairs Office

FORT GEORGE G. MEADE, Md. – COL Candy Boparai, commander, 780th Military Intelligence Brigade (Cyber), hosted a change of command ceremony whereby LTC Michael Krogh, commander, Operations Support Element, relinquished his command to MAJ John Rollinson at the Post Theater, June 15.

Although the first Cyber Solutions Development Detachment (CSD) was formally established in July 2017, the Operations Support Element, 780th MI Brigade (Cyber) is a new Army organization having been officially approved by the Department of the Army in July 2023 and formally recognized as the U.S. Army Intelligence and Security Command (INSCOM) Operations Support Element (OSE) on March 1, 2024.

OSE elements build, sustain, and provide teams to support the Cyber Mission Force's offensive cyberspace operations, develop operational capabilities, and enable utilization of cyberspace operations infrastructure.

COL Boparai stated in her remarks that OSE is often the first organization called, whether supporting offensive cyberspace operations for Joint Force Headquarters or the Cyber National Mission Force, or when delivering enterprise capabilities.

"This battalion operates at the speed of relevance," said Boparai. "The Soldiers and Civilians of OSE have demonstrated their expertise before the highest levels of leadership – including the Secretary of the Army, the INSCOM commander, and the Department of the Army G2 (Intelligence) – showcasing not only technical excellence, but professionalism and innovation that define this unit."

Boparai discussed LTC Krogh's leadership has been central to OSE's success.

"Your journey has been marked

by technical mastery and operational excellence. As a highly skilled Windows developer and technical expert, you brought unmatched understanding of the enterprise and the mission," said Boparai. "But more importantly, you enabled, you empowered, this organization to innovate, to solve hard problems, to forge new paths for the mission force. Under your command, OSE has codified CNODP (Computer Network Operations Developmental Program), created a pilot tool developer test, and developed a specialized pipeline for cyber teams focused on relevant, technical targets."

In his remarks, LTC Krogh talked about the OSE Soldiers and Civilians ingenuity, persistence, and drive.

"This unit's history is short, yet full of change. Our identity has always been something of a curiosity," said Krogh. "But it has never distracted us from the mission. The (Soldiers and Civilians) here are among the most impressive professionals I have ever had the privilege of working for. Their ingenuity, persistence, and drive have pushed the boundaries of what is possible. (You) represent and unprecedented collective talent who have risen to every occasion. Every time there seemed to be an unsolvable problem, they never backed down."

Introducing the incoming commander, MAJ Rollinson, COL Boparai told the audience that he is no stranger to the Brigade, coming from CSD – Georgia, where

his background in cyber operations, dedication to the mission, and his ability to build cohesive teams made him the "ideal leader for OSE's next chapter."

"Ubique Et Semper In Pugna"

"Everywhere and Always...In the Fight!" ■







781st MI Battalion (Cyber), Vanguard Change of Command

By 780th Military Intelligence Brigade (Cyber) Public Affairs Office

FORT GEORGE G. MEADE, Md. – COL Candy Boparai, commander, 780th Military Intelligence Brigade (Cyber), hosted a change of command ceremony whereby LTC Scott A. Beal, commander, 781st Military Intelligence Battalion (Cyber), Vanguard, relinquished his command to LTC Daniel S. Hawthorne, on the Parade Field, June 18.

As the Vanguard Battalion's companies stood in formation, in the time honored tradition of the United States Army, fellow Soldiers, friends and Family members gathered to bid farewell to one command team and welcome the another.

The 781st MI Battalion (Cyber), whose motto is *Ubi Ceteri Non Possunt*, Latin for 'When Others Cannot', presents the resources and capabilities from across the Army enterprise to man, train, and equip the Cyber National Mission Force (CNMF) to execute cyberspace operations to achieve operational outcomes against the adversaries of the United States.

"You have heard about the history of the 781st. Over the years, this battalion has grown in scope, scale, and complexity, consistently delivering effects where and when needed," said COL Boparai. "The 781st is unique: It is the Army's sole offensive cyber entity under the operational control of the Cyber National Mission Force, a distinction that underscores its critical role in national defense. You are the Vanguards – always at the front, always 'where others cannot.'"

She added that what the Vanguard Soldiers and Civilians accomplish is in the "shadows, far from the spotlight, but always at the forefront of our nation's security."

Whether responding to crises in the Middle East, countering aggression in Europe, or supporting operations along our Nation's southern border she stated the battalion's actions have shaped outcomes and protected lives.

"You serve in silence, and the things you do every day make the world safer – even if those things cannot always be spoken of. You truly go where others cannot," said Boparai.

COL Boparai stated the LTC Beal wore many hats. He served as the battalion commander, Service Component Command, and CNMF J7 Training Director. Under his leadership, the CNMF University was elevated, and new training courses and certification exercises were developed and taught. Over the past year, under Beal's leadership, the Vanguard achieved over 90 percent trained and qualified personnel, ensuring the 781st provided a ready force to the CNMF.

"Scott's legacy is one of operational excellence, technical innovation, and unwavering commitment to the Army, and the mission," said the brigade commander.

In his remarks, LTC Beal presented an impassioned speech about those he served with.

"Standing on this field today, looking out at the magnificent Soldiers in this formation, I am filled with an overwhelming sense of pride and humility to have led this battalion through our 250th anniversary of our Army and into the 250th anniversary of our country."

After thanking the distinguished visitors and guests; his Family (and most importantly his wife); COL Boparai; the Brigade Command Sergeant Major, CSM Joseph Daniel; his battalion senior enlisted leader, CSM Jack Hansen; his command group and command teams, company commanders and first sergeants; his battalion and brigade staff; he saved his most poignant remarks for the Vanguard Soldiers and Civilians.

After going through a litany of Soldier and Civilian names, reciting their achievements and honors, Beal

said "They are Citizen Soldiers, they are warrior scholars, and they represent the absolute best that America has to offer... They are parents, sons and their daughters, you are (all) absolutely amazing. You represent the best cross-section of our country. Although this ceremony has mine and LTC Hawthorne's name on the programs this is really for them. It's for you. You all made me successful in executing my intent and fulfilling my vision."

LTC Hawthorne comes to the Vanguard having previously served in intelligence, cyber, and academic roles, earning a doctorate in Digital Systems Security and authoring numerous articles and policies that have shaped Army doctrine.

"He brings a unique blend of technical expertise, operational acumen, and passion for innovation," said COL Boparai. "There could not be a more fitting leader to guide the 781st into its next chapter. Da, your reputation precedes you, and it is clear you are the right choice to take this battalion into the future."

Ubi Ceteri Non Possunt

"Everywhere and Always...In the Fight!" ■







The Joint Command and Control and Mission Command

By CPT Brendan Vito Stonionis, 781st Military Intelligence Battalion (Cyber)

THE ARMY'S PHILOSOPHY OF MISSION COMMAND is rooted in the German concept of Auftragstaktik, or mission orders, which emphasizes trust, initiative, and decentralized decision-making. Commanders provide subordinates with a clear purpose, desired end state, and intent, allowing them the freedom to solve problems on the battlefield. The Joint Command and Control (JCC2) system provides commanders with a centralized dashboard displaying soldier qualifications, training progression, personnel status, and readiness metrics. While JCC2 provides commanders visibility into readiness metrics, we risk conflating metrics with actual combat effectiveness. Our growing reliance on readiness dashboards and performance metrics risks undermining this philosophy. When commanders place greater trust in data than in the judgment of subordinate leaders, they inadvertently shift toward centralized control management. True mission command requires leaders to trust their people and exercise professional judgment, particularly in future conflicts where access to complete and accurate data may be limited.

JCC2 provides access to a trove of readiness information. A commander can quickly determine which Soldiers are qualified in required tasks, who has critical certifications, and display where training gaps exist. This visibility should in theory improve resource allocation, reduce administrative burden, and allow leaders to identify trends before they become significant readiness problems. JCC2 also improves accountability by allowing commanders to validate training completion, track personnel development, and ensure readiness requirements are being met across the CMF.

Despite these benefits, JCC2 creates a false sense of understanding. JCC2 may

indicate that a Soldier had completed required training, had necessary certifications, or met all measurable readiness standards. However, the dashboard cannot determine whether that Soldier can effectively perform under stress, adapt to changing conditions, or effectively contribute cohesively to the team. Leaders develop an understanding of their formations through daily interactions, training events, inspections, and operational experience. While subjective, these assessments often capture intangible factors such as morale, cohesion, leadership effectiveness, and adaptability that could never be captured on JCC2.

The availability of the metrics and dashboards that JCC2 provides creates an environment where leaders increasingly seek numerical validation before accepting assessments from subordinate commanders and leaders. Readiness is often reduced to percentages, color-coded charts, and arbitrary training requirements rather than a comprehensive evaluation of if that Soldier can do their job.

This tendency risks prioritizing what can be measured over what truly matters. Leaders may focus on improving dashboard statistics rather than increasing actual lethality. A unit may appear fully ready according to JCC2 while still lacking trust, cohesion, initiative, or tactical proficiency. The result is a readiness culture that rewards administrative compliance rather than combat effectiveness.

The Army's doctrine of mission command emphasizes trust, disciplined initiative, and decentralized decision making. Success in future operations will depend on leaders' ability to make decisions with incomplete information and rely on their judgment of subordinate leaders at all levels. An overreliance on systems such as JCC2 may unintentionally undermine this mindset by encouraging leaders to trust dashboards more than people. While

JCC2 can inform commanders, it cannot replace commander judgment. We must resist the temptation to equate readiness metrics with lethality and instead use data as one component of the readiness assessment. We need to re-instate mission command and view tools like JCC2 for what it is, a set of numbers and data that does not paint the entire picture. ■

Beyond the Checkbox: *Lessons from FMQ and What Proficiency Fit Must Get Right*

By CPT Daniel V. Alvarado, 781st Military Intelligence Battalion (Cyber)

I. The Shift Worth Taking Seriously

During her opening remarks at Senior Leaders Week, COL Candy Boparai, commander, 780th Military Intelligence Brigade (Cyber), stated that the Joint Cyber Command and Control (JCC2-R) “Fully Mission Qualified” (FMQ) metric is now to be used as a standard, not a target. Proficiency Fit is the new aim, where each team works toward meeting the Basic, Senior, and Master requirements for every work role it is authorized to fill. That guidance signals organizational maturity; it reflects a force willing to reexamine how it defines readiness and raise the bar rather than simply defend the one it already cleared.

The question worth sitting with is a harder one: how do we make sure we don’t repeat the same pattern with the next metric?

That is not a cynical question; it is an organizational one. Readiness metrics are not neutral instruments, they shape behavior, and when the right incentives are not aligned, they shape behavior in ways nobody intended. Before Proficiency Fit matures into the new guiding light, it is worth understanding what happened to the last one, not to relitigate it, but to draw the right lessons while the window is still open.

II. What FMQ Was Trying to Do and What Happened

For those who are familiar with JCC2-R and how it works, feel free to skip to the next paragraph. For the past year, the target was 80 percent FMQ for each team in the 780th MI Brigade. What this means is that 80 percent of the billeted members on a team must have completed all their pipeline training and completed their JQR (Job Qualification Record) for the work role they were slotted in, at the Basic level. Once both of those are done, that Soldier’s or Civilian’s status changes from “Pending”

to “Basic,” and they are now Fully Mission Qualified. How long this takes and how difficult it is depends on work role. Language Analysts have a short JQR and about four weeks’ worth of classes, so they can be FMQ in six weeks. An Exploitation Analyst (EA), on the other hand, has about twenty weeks of training, an extensive JQR, and several demonstrations requiring on-the-job training, so qualifying in a year is exceptionally quick.

FMQ made sense as a metric. It gave the Brigade a shared language for readiness, enabled cross-unit comparability, and created a forcing function that kept training completion honest rather than deferred indefinitely. In an environment where the gap between completing a pipeline and closing out a JQR can stretch across months, a metric that creates accountability for that distance is not nothing.

The problem was not that FMQ measured the wrong things. The problem was what happened when those measurements became the primary basis for evaluating leaders. The British economist Charles Goodhart observed in the 1970s what has since become a near-universal principle in organizational behavior: when a measure becomes a target, it ceases to be a good measure. This is not a failure of anyone’s intent. It is a predictable response to incentive structure. When leaders are evaluated on a number, they optimize for the number. The question is whether optimizing for the number also optimizes for the mission, and in the case of FMQ, several structural features made that alignment unreliable.

The first was PCS (transition) turnover. Consider a company starting at 100 percent FMQ, all 100 personnel qualified. If 30 new, unqualified personnel in-process in a single year and 20 FMQ personnel depart, the company ends that year at 62percent FMQ: 80 qualified Soldiers

over 130 total. Same training effort, same leadership, dramatically different number. Soldiers move; pipelines take time; the metric reflects a snapshot of a process no one fully controls. Leaders found themselves accountable for a number that was partly a function of assignment cycles set well above the unit level.

The second was scheduling dependency. The National Cryptologic University owns training throughput. Courses require six weeks’ advance notice. If an instructor is unavailable, the course may not reschedule. Commanders are held accountable for FMQ percentages but have limited authority over some of the conditions that determined them.

The third, and subtlest, was the JQR architecture. Joint Qualification Requirements are signed off by peers: once a Soldier completes a JQR, they can sign it for others who follow. The certification chain is self-referential by design and that does not make it fraudulent; it makes it a weak signal. A JQR sign-off tells you that someone completed the requirements as a peer understood them. It does not tell you what that Soldier can actually do. Across work roles, pipeline training is the bottleneck, either because it takes the longest to complete, or because part of the JQR requires it before demonstrating skills. By the time a JQR is signed, the question of whether that Soldier is capable has largely already been answered. The sign-off is a confirmation, not an evaluation. The certification functions like a receipt.

A fourth factor deserves mention. For years, Cyber Mission Force teams have been manned above authorization, a buffer that cushioned turnover and kept FMQ numbers achievable even during transition periods. That buffer is disappearing. A 2024 Army White Paper on “Army Force Structure Transformation” acknowledges the service is ‘significantly over-structured’ and directs reducing roughly 32,000

authorizations by FY2029, bringing force structure and end strength into closer alignment. The Secretary of Defense's April 2025 Army Transformation directive reinforces the mandate, calling explicitly for a leaner force optimized for maximum readiness. Cyber is not exempt from these pressures; no branch is. The metric did not change; the conditions that made it survivable did.

None of this is a new observation. The former Brigade Command Sergeant Major, James Krog, wrote in the September 2018 edition of the *Byte*, describing training pipelines as difficult and largely outside leader control, noting that what should take ten to twelve weeks can stretch to a year. MAJ Mark Klink's article in the same issue identified a deeper tension: organizations naturally focus on what gets measured and reviewed at higher levels, but in the Cyber National Mission Force construct, the operational command and service components are tracking different elements, Task Forces versus teams, creating a disconnect that made any single readiness metric an incomplete picture. Both pieces anticipated the present argument seven years ago. That the structural concerns they raised remain unresolved is itself evidence the system does not self-correct.

III. Proficiency Fit — What It Gets Right

To be direct: Proficiency Fit is a better metric than FMQ.

Not in every respect, but in the ways that matter most to an operational commander. FMQ treated all qualified operators as equivalent — a Soldier who finished their pipeline last week counted the same as one with three years of operational tempo behind them. Proficiency Fit breaks that equivalence by distinguishing Basic, Senior, and Master proficiency levels across each work role. A team of eight operators is not the same team when four are Basic and four are Master as when all eight are Basic. Proficiency Fit gives commanders a meaningfully more accurate picture of what a team can actually do.

The metric also accounts for team composition rather than raw headcount. Where FMQ measured qualified personnel

over billets, Proficiency Fit asks whether the people who are present fit the proficiency levels the team's work requires. That is closer to what a commander with a mission actually needs to answer.

These are not cosmetic improvements. They reflect a real advance in how the force conceptualizes readiness, a move from a binary qualified/not-qualified model toward something that captures depth and distribution of capability. The critique that follows is not skepticism of the new metric; it is an argument for protecting it.

IV. What to Watch — Proficiency Fit's Structural Vulnerabilities

Proficiency Fit rests on the same underlying architecture as FMQ. Most of the structural vulnerabilities described in the previous section do not disappear with the transition; they transfer, and in some cases sharpen, because the standard is higher.

The Assessment Chain

Where FMQ required one JQR at the Basic level, Proficiency Fit requires a JQR at each proficiency level (Basic, Senior, and Master) for each work role. The sign-off logic is the same: a Soldier who has completed the Senior JQR can sign it for others at that same tier. The self-referential structure does not disappear; it multiplies, and the certification layer above it was never designed to catch what the sign-off chain misses.

There is also a second layer of certification. The Team Lead, typically an O-4 or O-5 (officer rank structure), certifies JQR completions across every work role and proficiency level on the team. This is not a failure of those leaders; it is a design problem for the system. No one, regardless of technical background, can maintain the depth to evaluate performance across all work roles at all three proficiency levels simultaneously. In practice, a Team Lead is seeing this JQR for the first time after the trainer has signed off, but that trainer is the same peer-qualified Soldier described above, not an independent evaluator. The Team Lead's certification confirms the chain was followed, not that the chain sufficiently evaluated operational skills. The result is that the formal certification

layer does not add informational value; it adds administrative weight. Proficiency Fit percentages, like FMQ percentages before them, reflect how well units navigate a certification architecture, not how capable their teams actually are.

The Turnover Problem

Consider a team whose senior EA, a Master with years of operational experience, receives PCS orders. Either the next most-experienced EA fills their billet, and their previous billet goes empty, or the senior's billet is filled with a new trainee. The team's Proficiency Fit drops significantly, on a timeline set well above the unit level. Building a qualified bench has historically cushioned this gap, but as the manning buffer disappears, that cushion goes with it. When that drop carries professional consequences for decisions no one in the unit made, the metric is measuring circumstance, not leadership. The new metric raises the bar. It does not change who controls the ladder.

Goodhart, Again

The most important risk is the one this article is built around. If Proficiency Fit percentages carry the weight FMQ numbers did, the same optimization pressure will emerge. Teams will find the path of least resistance to the numbers. The clearest example is the one the system is most vulnerable to: when the number matters more than the capability, the pressure is to certify, not to develop. A JQR signed before its requirements are truly met raises the percentage without raising readiness, and under Proficiency Fit, that gap becomes more dangerous, because Senior and Master qualifications authorize riskier tradecraft than Basic. A falsely certified Basic Operator is a training problem. A falsely certified Master Operator is an operational one.

These are not arguments against Proficiency Fit; they are arguments for using it honestly. A Proficiency Fit percentage should inform the conversation about readiness, not end it.

V. What Readiness Actually Requires — The Harder Question

Both FMQ and Proficiency Fit measure inputs: courses completed,



FORT GEORGE G. MEADE, Md – U.S. Cyber Command operators participate in Cyber Guard 25-2 exercise on June 3, 2025, at Fort George G. Meade, MD. The exercise, in coordination with the Joint Staff, simulates scenarios that test response protocols and defensive and offensive techniques across geographic areas of responsibility. (Photo by: Skyler Wilson)

JQRs signed, proficiency levels achieved. Neither directly captures what a team does under operational conditions: the adaptive problem-solving when the target evolves mid-mission, the judgment under ambiguity that no curriculum fully addresses, the cohesion that holds when tempo increases and the team is tired. Measuring operational outcomes in a classified environment is difficult, and a force that waited for perfect metrics before tracking anything at all would track nothing. But a number that tells you what Soldiers have completed cannot tell you what they can do. Training metrics are necessary, but they are not sufficient. The certification architecture tells us something about the population of trained Soldiers; it does not tell us, and is not designed to tell us, whether teams are ready in the ways that matter when it counts.

The U.S. Cyber Command JQR revision effort is evidence that the force is already asking these questions. That work deserves broad participation and a critical eye focused not just on whether proficiency is assessed, but on what it

means for proficiency to be real.

What readiness ultimately requires, and how to build a measurement system that captures it, needs perspectives and authorities beyond what a single echelon can see. The question this article is raising belongs to everyone in the Brigade as well as senior leaders and organizations above it who own the systems being measured.

VI. The Opportunity in the Transition

When a team has strong FMQ or Proficiency Fit numbers, it is usually because of something the metric cannot capture: a culture of accountability, leaders who develop their people, Soldiers who take ownership of their own readiness. The numbers are downstream of those things. The risk is mistaking the reflection for the source.

The shift from FMQ to Proficiency Fit is an opportunity, and timing matters. Metrics are easier to shape before they calcify into the primary basis for evaluation. The moment to ask hard questions is now, before the optimization pressure arrives.

Three things would make Proficiency

Fit more durable than FMQ. First, some form of scheduling authority, or at minimum a meaningful recovery option, for commanders whose numbers drop from circumstances outside their control. Second, company-level input into what Soldiers at each proficiency level should actually be able to accomplish, so JQR requirements track operational reality rather than administrative consensus. Third, a shared commitment across this readership to hold the metric loosely: as a useful data point rather than a verdict on the teams and leaders behind it.

None of those are simple asks, and all of them are worth the conversation.

The question this article wants to leave open: as we build toward what Proficiency Fit is asking of us, what would it look like to know (not certify, but actually know) that a team is ready? ■



A Unified Front: *How the 780th MI BDE Delivers Holistic Cyber Readiness*

By SGT Jaysen Johnson, Detachment Texas, 782d Military Intelligence Battalion (Cyber)

THE BATTLE FOR THE electromagnetic spectrum and cyberspace begins long before the first kinetic strike. In this complex domain, victory is not determined solely by the sophistication of our tools, but by the readiness of the operators behind the keyboard. As the Army's sole offensive cyber operations brigade, leveraging more than 2,400 personnel across four states, the 780th Military Intelligence Brigade plays a pivotal role in national defense.

Delivering "ready combat formations" is the strategic center of gravity for the Cyber Mission Force (CMF). However, generating these formations is not merely a tactical endeavor. It requires a synchronized, holistic approach to readiness that spans all four of the Army's focus areas: warfighting, delivering ready combat formations, strengthening the profession, and continuous transformation. By fusing administrative discipline, advanced technical schooling, and tactical operational execution, the Brigade ensures its forces are prepared to meet U.S. Army Cyber Command's vision of fighting in contact now while building for future conflict.

The Foundation: Talent Management and Administrative Discipline

Before a cyber operator can maneuver within an adversary's network, they must first meet the rigorous standards of being a United States Army Soldier or Army Civilian. This foundational readiness begins with robust talent management and administrative discipline across the battalion.

As COL Candy Boparai, commander of the 780th MI Brigade (Cyber), has noted, "The Army's most significant inputs into cyber readiness are presenting high quality personnel and providing the supporting talent management policies to sustain them in Cyber Mission Force long enough to achieve and maintain mastery in their skillsets."

Administrative readiness is operational readiness. Maintaining consistently high compliance rates in mandatory training, medical readiness, and security clearances is

the prerequisite for operational authorization. This is exceptionally challenging given the geographic dispersion of the Brigade. For instance, the 782d MI Battalion (Cyber) is headquartered at Fort Gordon, Georgia, but has operational detachments in Hawaii and Texas. Synchronizing readiness metrics and school allocations across multiple time zones requires immense precision from the battalion staff.

Consider the recent technical disruptions to the U.S. Cyber Command Joint Cyber Command and Control Readiness (JCC2-R) system. Rather than allowing training to stall, battalion support staff and JQR proctors rapidly implemented a temporary transition to paper Job Qualification Requirements. This swift administrative pivot ensured the qualification pipeline remained fully operational, demonstrating how agile, behind-the-scenes support directly sustains operational momentum.

Scaling Force Structure and Continuous Transformation

The Brigade is not just maintaining steady-state operations; it is actively growing to meet emerging threats. Training pipelines must scale alongside this operational capacity.

Recently, the 782d MI Battalion (Cyber) consistently exceeded expectations in support of national security objectives by enabling two new CMF teams to reach Full Operating Capability (FOC) and developing a brand-new training scenario for mission readiness events. This mirrors broader Brigade growth, such as the activation and FOC achievement of C Company, 11th Cyber Warfare Battalion. Ensuring these new formations are fully equipped, trained, and legally compliant requires a monumental, synchronized effort from headquarters staffs and support elements across the enterprise.

Advanced Schooling and Tactical Execution

With foundational requirements secured, the focus shifts to maintaining technical mastery. As LTC Matthew Hutchison, commander of the 782d MI Battalion

(Cyber), remarked upon taking command, "Today's current operating environment gives cyber forces little respite from the stresses of sustained training and operations. However, I look forward to working as a team to pursue mastery in our craft and continuing to take measured steps to be the most well-trained and adaptable cyber forces supporting the Joint Force."

This pursuit of mastery is guided by data-driven operational needs. Recent Army Defensive Cyber Operations (DCO) prioritization efforts have produced HQDA-sanctioned, field-informed requirements for the coming fiscal years. By aggressively forecasting school seats and aligning training tracks with these validated DCO missions, the battalion ensures operators are matched to the specific technical demands of the modern battlespace.

The culmination of this holistic pipeline is tactical execution. When Combat Mission Teams and Cyber Protection Teams deploy, they operate with the confidence that their logistical, administrative, and training support is fully secured.

Conclusion

"You train like you fight," emphasized LTG Maria Barrett, former commanding general of U.S. Army Cyber Command. "So, every experimentation, every CTC rotation, every warfighter, we need to be inserting real-world scenarios."

Executing that mandate requires a unified front. The integration of administrative discipline, talent management, and tactical execution is what enables the 780th MI BDE (Cyber) to dominate the cyber domain. Building these formations is a collective endeavor that relies equally on the diligent support of the battalion headquarters and the technical expertise of the operator on the keyboard. By maintaining this synchronized ecosystem, the Brigade ensures the Cyber Mission Force remains ready to disrupt adversaries, defend the nation, and win in cyberspace.

References:

1. Army.mil article on the Principal Cyber Advisor's August 2025 visit (Brandon Pugh)
2. The 780th MI BDE's The BYTE Vol. 13, Issue 4 (Lethality: Training and Readiness)
3. Army.mil article on the 782d MI BN change of command (June 4, 2025)
4. ARCYBER's ADCyOC 2025 article on DCO prioritization
5. LTG Barrett's TechNet Augusta 2025 remarks (via Breaking Defense) 





The Revised Cyber Force Generation Model: A Framework for Operational Readiness

By CW2 Melanie Wahl and Mr. Mike Holdway, 508 Combat Support Team, D Company, 782d Military Intelligence Battalion (Cyber)

Introduction

THE EVOLUTION OF THE ARMY CYBER MISSION FORCE enables the Brigade to align readiness with the demands of cyberspace operations. The Revised Cyber Force Generation Model provides a clear path to transition from traditional readiness metrics to a cycle that emphasizes operational availability. This framework helps the Brigade maintain trained and ready formations that support national objectives. The current operational environment requires a force that generates combat power through a disciplined, predictable cycle. This shift reflects a more sustainable approach to building and delivering combat-ready formations to the Joint Force. It also supports prioritizing the Warfighter by recognizing that adversaries have already engaged in the competition phase.

Strategic Opportunity within Force Generation

The Revised Cyber Force Generation Model introduces a structured methodology that maximizes the Brigade's ability to employ Cyber Mission Forces globally. By moving away from ad hoc tasking, the model emphasizes deliberate progression through training and certification to validation, operational employment, and sustainment. Adjusting the model gives leaders a clearer view of unit capabilities and allows early identification and correction of gaps. Implementing this framework creates predictable mission cycles, encourages innovation, and strengthens cyber operations mastery. This structured cycle also supports sustained cyber operations across the conflict continuum.

Phase One: Foundation and Collective Training

Phase I focuses on developing foundational skills and collective readiness. It provides an opportunity to integrate

personnel into established teams and reinforce the competencies required for continuous and complex cyber operations. The phase emphasizes synchronizing individual technical skills with team-level maneuver. Combat formations perform best when Soldiers understand their roles and how they support mission success.

The revised model ensures Job Qualification Requirements (JQR) move beyond checklist-based training by prioritizing mission performance and measurable results. Trainers must confirm that Soldiers demonstrate proficiency through hands-on execution and understand task dependencies and real-world application. Leaders should evaluate tasks through mission operations when feasible and leverage organic resources to identify additional tradecraft opportunities.

This phase also requires leaders to standardize TTPs (tactics, techniques, and procedures) and develop SOPs (standing operating procedure) through continual refinement. These standards ensure we are training for the threat, not a checklist. Deliberate training in Phase I builds the skills and processes teams rely on during later operational employment.

Phase Two: Certification and Validation

Certification verifies a team's ability to meet Mission-Essential Tasks and ensures alignment with standards established by Army Cyber Command and U.S. Cyber Command. This includes assessing internal team coordination, technical execution, and role-specific contributions. Validation confirms performance under realistic operational conditions. Validation exercises replicate the pressures, ambiguity, and joint requirements characteristic of cyberspace operations. These exercises allow teams to operate within Joint All-Domain Operations (JADO) frameworks, testing their resiliency and cohesion. Success in

Phase II reassures commanders that teams are prepared to fight and win across the cyberspace domain in competition, crisis, or conflict. Transparency during this process gives teams accurate assessments to refine TTPs and SOPs before employment.

Phase Three: Operational Employment and Persistence

Phase III represents the culmination of the force generation cycle. During this phase, leaders assign teams to mission sets in support of theater or national objectives. The model ensures that teams enter the operational environment at peak readiness. A sustained presence enables teams to maintain access, track adversary activity, and provide commanders with relevant intelligence.

Operationalizing this cycle provides mission partners with consistent and reliable support. Regular engagement with mission partners enhances tradecraft development and strengthens community-wide understanding of the operational environment. Real-world mission feedback informs adjustments to future training plans, helping refine both individual and collective readiness. Operational employment is where training, certification, and validation translate into tangible effects for the Joint Force.

Integration with Joint All-Domain Operations

Cyber capabilities are most effective when synchronized with operations across land, air, maritime, space, and information domains. The force generation model provides the structure to align cyber readiness cycles with the training and deployment schedules of other Army formations. This synchronization ensures commanders have access to cyber capabilities that complement decisive operations. Participation in large-scale exercises during Phase II enhances interoperability and supports integrated

JADO.

Leadership Roles within Model Execution

The Revised Cyber Force Generation Model's success depends on strong leadership at echelon. Leaders must commit to the discipline the cycle demands and shift from reactive tasking to proactive planning. Leaders are responsible for ensuring training environments are realistic, standards remain high, and missions are clearly defined. The model allows leaders and technical experts the freedom to cultivate required skills within the digital domain,

prioritizing mastery over manpower. When leaders prioritize the integrity of the force generation process, the organization becomes more adaptable and prepared to meet ever evolving requirements. The result of this process is a more prepared force able to meet operational demands.

Conclusion: Delivering the Future Force

The Revised Cyber Force Generation Model represents a significant opportunity for the Brigade and the broader Cyber Mission Force to shift toward operational mastery. By emphasizing foundational

training, objective certification and validation, and persistent operational employment, the model strengthens the Army's ability to operate effectively in cyberspace. This framework aligns with U.S. Cyber Command's mission and supports the needed evolution to ensure capable cyber force. As the Brigade prepares for future conflict, this model provides a cyclic approach for generating and sustaining combat power in the digital domain. ■





Army Cyber Capability Developers and Cyber Warfare Battalion Collaborate on Drone Dominance

By SPC William Perez, Cyber Capabilities Developer, Hardware Section, CSD-Maryland, Operations Support Element, 780th Military Intelligence Brigade (Cyber)

FORT GORDON, Ga. – Developers from the Hardware Section of CSD-Maryland (Cyber Solutions Development), 780th Military Intelligence Brigade (Cyber), recently collaborated with developers from the 11th Cyber Warfare Battalion's CSD-Tactical on a project to increase the Army's drone warfare capabilities.

The project, which spanned more than a year, aligns with the Army's "Transforming in Contact" initiative, which aims to modernize the battlefield by rapidly delivering new technology into the hands of Soldiers. Drone warfare has become one of the most significant battlefield innovations in recent years, with several countries scrambling to develop increasingly advanced drone technology following the outbreak of the war in Ukraine.

This project required developers to work across several technical domains, including embedded systems, RF engineering, 3D printing, networking systems, and more. Developers from CSD-Maryland collaborated with CSD-Tactical through shared Git repositories, hundreds of remote meetings, and numerous TDY trips.

The project culminated with a visit to U.S. Army Cyber Command (ARCYBER) by the Secretary of the Army, Honorable Daniel P. Driscoll, on March 26. CSD-Maryland's Hardware Section traveled to Fort Gordon, Georgia, to demonstrate the numerous capabilities developed over the previous year. The drone demonstration was conducted alongside the 11th CWB's Expeditionary Cyber and Electromagnetic Activities (CEMA) Teams (ECTs) which showcased their ability to provide battlefield lethality through cyberspace operations. Developers from CSD-Maryland demonstrated to the Secretary Driscoll, LTG Christopher L. Eubank, commanding general, ARCYBER,

and other senior leaders their ability to simultaneously deploy three autonomous 3D printed VTOL (Vertical Take-Off and Landing) drone systems and corresponding software solutions developed entirely in-house.

This project, which originated at CSD-Maryland, was fully transitioned to the 11th CWB shortly after the demonstration, enabling the battalion to continue developing and employing the capability. The impact of this effort extends beyond cyber units. The project was designed not only for use by ECTs within the 11th CWB, but also for potential employment by Army Brigade Combat Teams. This demonstrates how the gap between cyber operations and more traditional combat roles continues to

narrow as battlefield technology becomes increasingly advanced.

This evolving battlefield environment makes the task of building combat-ready formations more important than ever, whether through the development of new battlefield capabilities by organizations such as CSD-Maryland and CSD-Tactical or through training in cyber warfare tactics by ECTs. By remaining at the forefront of emerging wartime strategies, including drone warfare and expeditionary cyber operations, the Army's cyber forces are helping ensure that Soldiers remain prepared to face any adversary in an increasingly complex and dynamic operational environment.





FORT GORDON, Ga.— Developers from the Hardware Section of CSD-Maryland (Cyber Solutions Development), 780th Military Intelligence Brigade (Cyber), recently collaborated with developers from the 11th Cyber Warfare Battalion’s CSD-Tactical on a project to increase the Army’s drone warfare capabilities.

The project, which spanned more than a year, aligns with the Army’s “Transforming in Contact” initiative, which aims to modernize the battlefield by rapidly delivering new technology into the hands of Soldiers. Drone warfare has become one of the most significant battlefield innovations in recent years, with several countries scrambling to develop increasingly advanced drone technology following the outbreak of the war in Ukraine.

U.S. Army photos contributed by CSD-Maryland, Operations Support Element, 780th Military Intelligence Brigade (Cyber) ■



Preparing Cyber Formations for Tactical Operations

By CPT Curtis Peters, A Company, 11th Cyber Warfare Battalion

CYBER PROTECTION TEAMS (CPTS), NATIONAL MISSION TEAMS (NMTS), AND COMBAT MISSION TEAMS (CMTS) were designed to execute highly specialized cyberspace operations in support of national-level objectives. These formations combine technical expertise and mission-focused capabilities to achieve strategic cyberspace effects in support of national security priorities. These formations have proven highly effective in achieving strategic cyberspace objectives. However, the evolving operational environment and modern battlefield now require cyber capabilities that can support maneuver forces at the tactical edge. Extending cyberspace effects into dispersed and contested environments demands a new organizational mindset, decentralized leadership philosophy, and adaptive operational processes. To meet this demand, tactical cyber formations must embrace mission command principles that empower junior leaders to execute

cyberspace operations independently while remaining aligned with commander's intent. This article discusses leadership concepts, operational processes, and training methodologies that assist in developing tactical cyber formations capable of operating effectively in decentralized environments.

Unlike traditional cyber mission structures, expeditionary cyber formations must operate in a far more decentralized manner. The principles outlined in Army Doctrine Publication (ADP) 6-0, Mission Command, provide an effective framework for enabling tactical cyberspace operations. Mission command empowers leaders at lower echelons to execute complex operations independently while remaining aligned with commander's intent, operational guidance, and legal authorities.

These principles establish the foundation for trust, shared understanding, disciplined initiative, and prudent risk acceptance throughout the formation. In practice, this requires deliberate training models,

decentralized execution, and clearly established operational expectations that prepare tactical leaders to operate effectively in dynamic environments.

The 11th Cyber Warfare Battalion's (CWB) Expeditionary CEMA Team (ECT) training model in Figure 1 provides an example of how mission command principles can be integrated into tactical cyber training and operational readiness. Tactical leaders are often positioned closest to evolving operational conditions and are best suited to assess mission requirements in real time. Providing those leaders with the flexibility to exercise disciplined initiative is critical to operational success, decentralized execution, and long-term leader development. A Company, 11th CWB, has implemented training guidance and operational products specifically designed to reinforce decentralized execution, tactical readiness, and collective mission understanding across expeditionary cyber formations as shown in Figure 2 and 3.

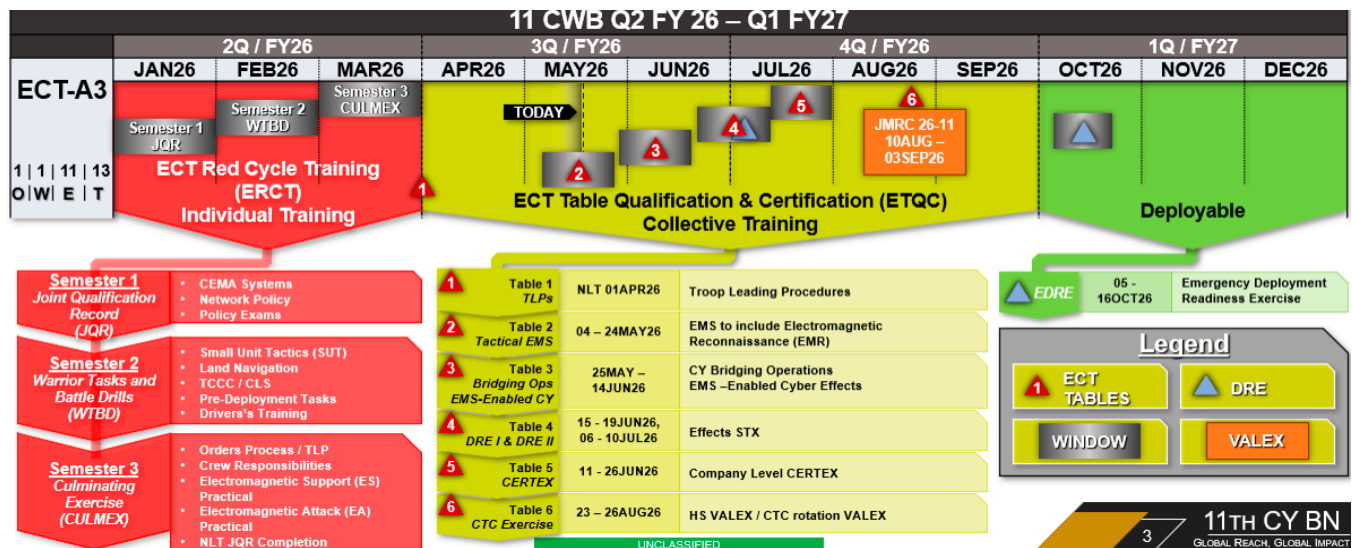


Figure 1: 11th CWB Expeditionary CEMA Team Qualification and Certification Progression.

Leviathan Big Seven 1. Shoot (Familiarization and Qualification: M17, M4) 2. Move (Land Navigation, Mounted and Dismounted Tactical Movement) 3. Communicate (Radio Operation, Reports, Brevity Codes) 4. Survive (Buddy Aid, Combat Lifesaver) 5. CEMA (Expeditionary CEMA Qualification Tables, Joint Qualification Requirements (JQR)) 6. Deploy (Soldier Readiness, Command Deployment Discipline Programs) 7. Thrive (Resiliency, Family Readiness, Financial Readiness) BN Annual Training Guidance Here ECT TACSOP Here	Company Training Guidance: Talking Points - Team Leads will take charge of training schedule. - Lead company training meetings and optional training syncs at team level - Brief WARNOs and OPORDs for every training event to their teams - ECTs will maximize field time for both technical and tactical training. - Field training will utilize training aids as often as possible (target emitters, artillery simulators, blanks, dummy rifles as a last resort). - Tactical training will use the BN ECT TACSOP as a reference. - Teams in red cycle will plan company wide PT tests, range, and readiness events. - Teams in amber cycle will focus on collective technical and tactical field training event. - Teams in green cycle will maximize family time while at home station.
---	--

Figure 2: A Company Tactical Cyber Training Guidance

No Fail: Joint Qualification Record (JQR)	No Fail: BN Tables 1-6	No Fail: Mission Execution
- EW Equipment Training - Beast - Kraken - RADDs - Cape Section Systems - Drivers Training - Weapons Qualification/PT Tests - Additional Duties/Schools - Tactics: Situational Training Exercises (STX)	- Team Validations - Crew Certifications - CULMEXs - Soldier Readiness Program (SRP) 1/2 - Deployment Readiness Exercises (DRE) - Collective Training Events (Technical with Tactical)	- Mission Planning and Preparation - Rehearsals - Sand Table Exercises - TTP analysis/application - Maintain deployment readiness - Medical Readiness 350-1 Training - Equipment / CEMA Slant - Packout requirements - Collective Training Events (Tactical with Technical)

Figure 3: Company Tactical Cyber Readiness and Training Framework



The Army expects cyber formations to operate effectively across all domains, including contested and dispersed tactical environments. As cyberspace capabilities continue to expand in support of maneuver operations, tactical cyber formations must remain agile, disciplined, and capable of decentralized execution. Mission command provides the leadership framework necessary to empower subordinate leaders while maintaining unity of effort across the formation. Through deliberate training, operational trust, and decentralized leadership, tactical cyber formations can successfully extend cyberspace effects to the tactical edge while supporting the broader objectives of joint and multidomain operations. These principles reinforce the importance of leader development, communication, and adaptability within tactical cyber units operating in rapidly changing environments as shown in Figure 4.

The continued evolution of tactical cyberspace operations will require adaptable leaders, resilient teams, and organizations capable of operating effectively in complex operational environments as shown in Figure 5. Developing these formations today ensures the Army remains prepared for the operational challenges of tomorrow. Continued investment in training, modernization, and integration with conventional forces will strengthen the Army's ability to synchronize cyber capabilities across future operations.



Figure 4: 11th CWB tactical leaders give direction and set expectations during field training exercise convoy brief.



Figure 5: A Company, 11th Cyber Warfare Battalion Soldiers conducting JQR progression and tactical training in preparation for team validation scheduled for late 2026. ■

The Road to Drone Dominance: *Drones without the Dollars*

By 1LT Omkar Kale, B Company, 11th Cyber Warfare Battalion

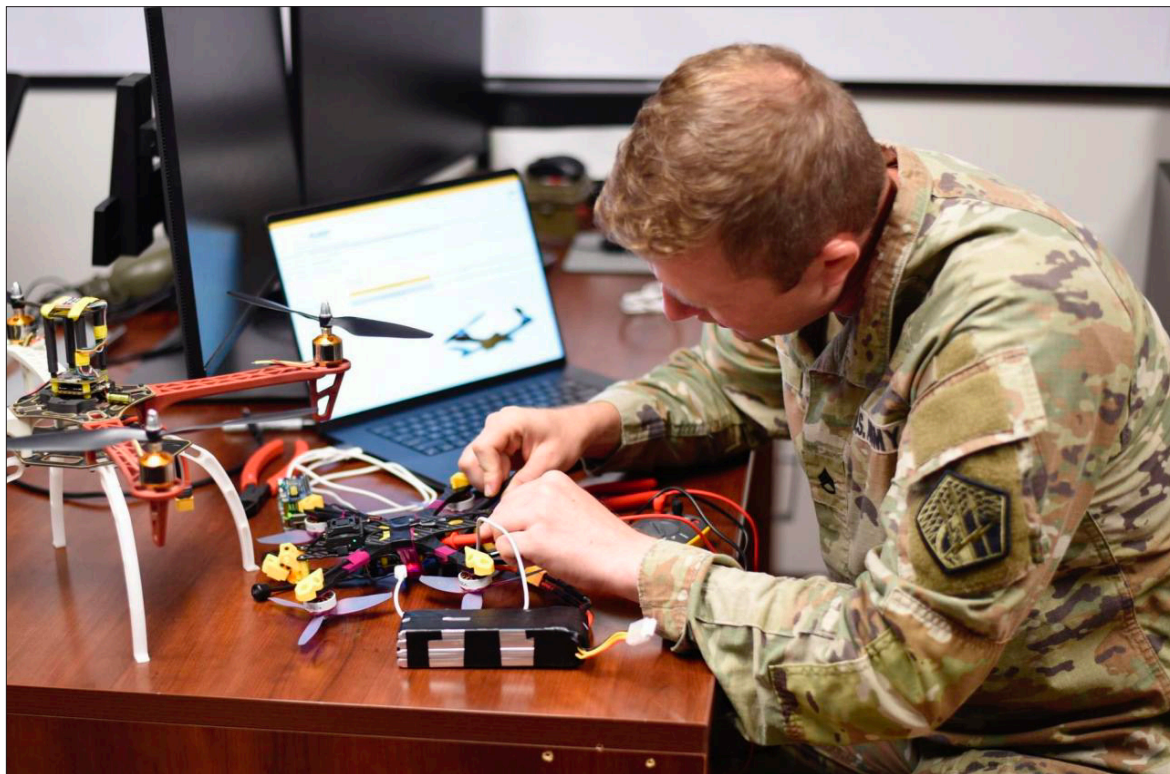
THE UNITED STATES ARMY relies on the ability to adapt and improve its strategy on the fly to best tackle conflicts around the world. In a modern combat environment where adversaries can be counted on to constantly probe our facilities and infrastructure while rigorously defending their own, bringing the best equipment for a situation ensures that we can meet our mission requirements. One of the ways units can stay relevant in today's environment is by integrating flexible drone platforms able to conduct multi-domain operations.

Drones have already shown their value in gathering intelligence, and the war in Ukraine has shown the effectiveness of using kamikaze drones against high value targets. In the hands of a Cyber unit, drones can provide a decisive advantage

by conveying cyber effects across greater ranges. However, current iterations of drones marketed to units pose a series of problems: they are expensive, hard to repair, and require specific training for each system. This poses problems for any long-term employment strategy; how do we keep drones operational, provide meaningful training, and conserve costs when a single aerial mishap can cause weeks of delays and thousands of dollars in repairs? The answer to this problem lies in local, in-house development of drone platforms. By avoiding third party procurement, The Army can better address the equipment costs and lengthy maintenance that plague drone employment.

In the past few months, drones have become one of the main focal points of development at 11th Cyber Warfare

Battalion. Inspired by the Department of War's Unleashing Drone Dominance program, Soldiers and teams, particularly in the 11th CWB Development Section, have been focusing on their own small projects with the goal of having their design employed on a larger scale. Everything from traditional quadcopters to hybrid glider designs are on the table, and interest across the battalion continues to grow. This type of development has two key benefits. The first is cost reduction; within 11th CWB, sections have been creating their own parts utilizing 3D printing and open-source technology, such as BetaFlight, to allow for rapid and cheap prototyping. This prevents reliance on third party distributors by empowering teams to do their own repair and modification of drone frames, saving time and money. The second is flexibility;



FORT GORDON, Ga. – An 11th CWB Soldier working on a training drone and FPV camera.



teams have the freedom to explore unorthodox designs suited to different kinds of missions and create their own solutions to problems such as payload limitations, loiter time, and energy usage. This also allows teams to create drones tailored to specific missions, rather than relying on one procured platform to be a jack of all trades.

This kind of development still has its own hurdles. SSG Cory Fox, an ECT crew lead at B Company and FAA-licensed Unmanned Aerial Systems pilot, described the problem with development, “The bottleneck [for development] is where do we get the integrated flight controllers, gyros, altimeters and accelerometers? These pieces of hardware pose a cost limitation, and we can’t use foreign systems for some parts.” With companies like DJI offering the same parts for cheaper, it can be hard to find domestic manufacturers willing to take on complex manufacturing without

charging exorbitant prices.

The solution, he elaborates, may lie with how we are trained; “The biggest way to eliminate this gap [in procurement] is to increase training time and thus reduce reliance on expensive sensors and Chinese made flight guidance systems”. He points to specific examples of mass-produced FPV drones being used in Ukraine and Lebanon, pointing out that many systems are manually flown. This kind of control scheme requires significant training but eliminates the need for costly sensors. Low cost training software, such as Tryp, a physics-based drone simulator available through the Steam Digital Storefront, prepares operators for the demanding job of piloting drones by hand without putting hardware and personnel at risk. Other units, such as 82nd Airborne, have pioneered more inexpensive real world training plans, creating enclosed drone training areas that can be used by Soldiers

at any time, circumventing the need for airspace deconfliction and spectrum planning. These techniques make training more accessible, allowing units to schedule more training for operators without the usual obstacles to planning.

In summary, internal initiatives for manufacturing drones provide more cost effective, tailored solutions. Initial efforts have already shown that it is possible to develop modular drone chassis at the unit level. While bottlenecks do exist when it comes to procuring assisted flight controllers and sensor packages, some of the supply issues can be circumvented with affordable, openly available training solutions. By bringing drones to the unit level and empowering units to experiment, we can increase the operational time and minimize downtime for these systems, increasing overall unit readiness and bringing teams closer to drone dominance. ■







Command Chief Warrant Officer James Richards Retires After 24 Years of Army Service

By 780th Military Intelligence Brigade (Cyber) Public Affairs Office

WASHINGTON – Chief Warrant Officer 5 James Richards, formerly the Command Chief Warrant Officer for the 780th Military Intelligence Brigade (Cyber), retired after more than 24 years of Army service in a Department of the Army Retirement Ceremony in Conmy Hall on the historic installation, Joint Base Myer-Henderson Hall, May 14, 2026.

CW5 Richards hails from Glendora, California, and enlisted into the 311th Theater Signal Command, U.S. Army Reserve on March 20, 2002, at Fort George G. Meade Military Entrance Processing Station. Richards received his commission as a second lieutenant from the U.S. Officer Candidate School on December 4, 2002; and attained a BA in Computer Science from Cornell University in 2002. He resigned his commission and received a direct appointment as a warrant officer on August 18, 2006, while serving in the Delaware Army National Guard.

“His achievements leave a legacy of enabling the Cyber Mission Forces (CMF) and the U.S. Department of War (DOW) cyber enterprise to achieve historic milestones, unlock the force’s potential to act, and build a path for individuals of all Services to reach their full potential,” said COL Candy Boparai, commander of the 780th MI Brigade (Cyber). “CW5 Richards was a pioneer and trailblazer in U.S. Cyber Command (USCYBERCOM), establishing or directing the creation and first use of many elements of the Cyberspace Operations enterprise that are routinely employed today.”

In 2016, CW5 Richards was the mission commander for one of the first USCYBERCOM missions that exercised two of the military cyberspace collection authorities, enabling thousands of operations per year since then. He also

designed the initial oversight training for one of those authorities, permitting the CMF to proliferate use of the authority across the enterprise. He guided the operational design of multiple cyberspace operations campaigns. Additionally, in 2020 he was the tactical planner for the first cyberspace effects operation conducted by a Cyber National Mission Force (CNMF) Joint Task Force which involved three crews of people executing operations for more than 60 hours. Outside of operations, during his time as a Mission Director in USCYBERCOM’s J3 (operations), he led efforts to establish policy that more closely included allied personnel as full participants in the enterprise, employ multiple authorities simultaneously on the same operation, allow Information Operations to leverage the full range of permissible actions under cyberspace operations, and leverage master-level members of the CMF to individually assess and mitigate previously unknown risk while on operation.

His leadership during the formative years of USCYBERCOM helped create the conditions for it to mature its own platforms and routinely execute operations that blend known uses of authorities with disciplined risk acceptance to maintain the DOW’s strategic overmatch against our adversaries.

CW5 Richards was a steward and builder of the CMF’s workroles, CMF training, and the Army’s implementation of them. In 2018, he was one of the architects of the first revisions in the qualification standard for two workroles since their establishment: Mission Commander and Exploitation Analyst. Additionally, with a small group across the CMF, he rebuilt the Mission Commander Course (MCC) to include modern elements of cyberspace operations, authoring three out of 18 modules personally and training over 400 Mission Commanders over the next six years as one of the primary

instructors for the course. The course additionally served as the basis for Mission Commander training that is conducted at the U.S. Army Cyber School, Fort Gordon, Georgia, today. To bring these and other CMF workroles into the Army’s personnel systems, he also worked with multiple elements at U.S. Army Cyber Command and the Cyber Center of Excellence over the course of more than six years to establish a series of Primary Developmental Skill Identifiers (PDSI) and modernize the Cyber Assignment Incentive Pay (CAIP) program, culminating in a major corrective revision in April 2025 that brought the programs in line with current CMF workroles and readiness requirements. In conjunction with those changes, he championed the expansion of utilization tours for recipients of Training With Industry (TWI) and Advanced Civil Schooling (ACS) benefits from approximately five positions across 780th MI Brigade (Cyber) to more than 25, covering every location the Brigade has personnel for the first time in its history. Also, during his tenure as the first Army warrant officer (WO) to serve as a Mission Director in the USCYBERCOM J3, he refined the qualification standard for that role and trained the next four Mission Directors, including the next two Army WOs to hold the role.

Beyond his work within the Cyberspace Operations enterprise, CW5 Richards contributed his expertise to strategic efforts. From 2021 to 2024, he was one of three Cyberspace Operations advisors to the Office of Net Assessment’s global exploratory exercise series, and one of the designers of its mechanism to incorporate cyberspace effects into those exercises. Leveraging more than eight years as a plankholder in the Army’s Cyber Warrant Officer Cohort, from 2022-2024 he advised the Headquarters, Department of the Air

Force, A1 and the 16th Air Force as it re-established Warrant Officers in the US Air Force, culminating in the first 30 US Air Force Warrant Officers being appointed in over 66 years at Maxwell Air Force Base in December 2024.

“From CMF Team to Combatant Command, and from the classroom to the operations floor, CW5 Richards’ leadership and expertise have left a lasting impact

on the Cyber Mission Forces, the DOW Cyberspace Operations enterprise, and the US Army,” said Boparai.

CW5 Richards may be leaving the Praetorian and Army family; however, his legacy and impact will be remembered in the years to come.

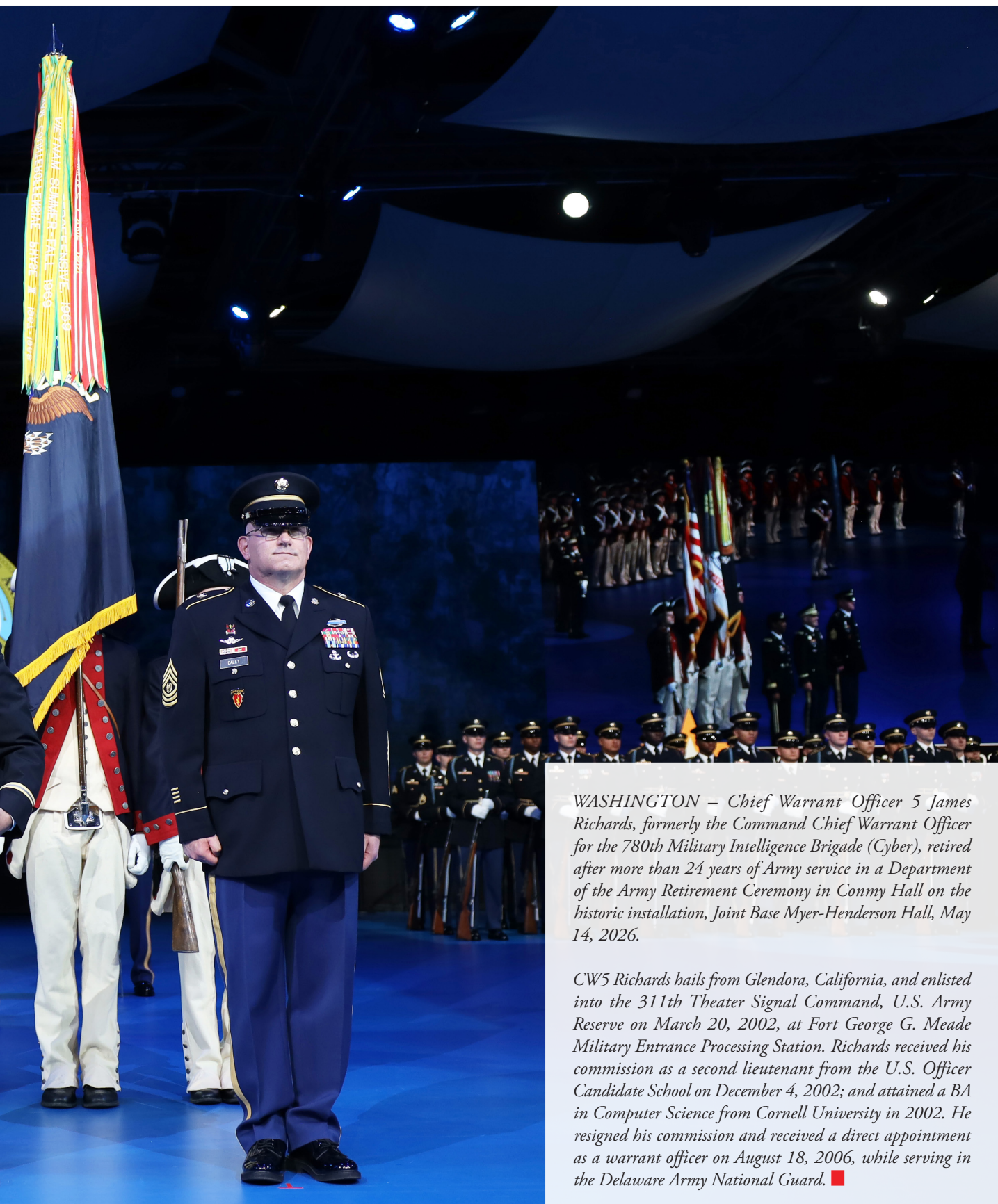
“24 years in the Army taught me that helping others is not a zero-sum game. Throughout your career, people will lift

you up so you can go back and lift others up yourself,” said CW5 Richards. “Use the chances they give you to understand other people – even the ones who oppose you – and you might find that they are just the kind of people you want to help, and not adversaries at all.”

*“Ubique Et Semper In Pugna”
“Everywhere and Always...In the Fight!”*







WASHINGTON – Chief Warrant Officer 5 James Richards, formerly the Command Chief Warrant Officer for the 780th Military Intelligence Brigade (Cyber), retired after more than 24 years of Army service in a Department of the Army Retirement Ceremony in Conmy Hall on the historic installation, Joint Base Myer-Henderson Hall, May 14, 2026.

CW5 Richards hails from Glendora, California, and enlisted into the 311th Theater Signal Command, U.S. Army Reserve on March 20, 2002, at Fort George G. Meade Military Entrance Processing Station. Richards received his commission as a second lieutenant from the U.S. Officer Candidate School on December 4, 2002; and attained a BA in Computer Science from Cornell University in 2002. He resigned his commission and received a direct appointment as a warrant officer on August 18, 2006, while serving in the Delaware Army National Guard. ■



HHC (Hastati), 780th MI Brigade (Cyber) Change of Command Ceremony





FORT GEORGE G. MEADE, Md. – Lieutenant Colonel Matthew, D. Heinmiller, Deputy Commander of 780th Military Intelligence Brigade (Cyber), hosted a change of command ceremony whereby Captain Mary A. Watkins relinquished her command of the brigade's Headquarters and Headquarters Company, Hastati, 780th MI Brigade (Cyber), to Captain Amanda K. RoperBrooks at the McGill Training Center Ballroom, June 4.

"Facta Non Verba" ■





MISSIONE PRO7

CISA Announces Winners of the 2026 President's Cup Cybersecurity Competition

Seventh Annual Competition Highlights Top Cybersecurity Talent in the U.S. Government

WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA) announced the winners of the seventh annual President's Cup cybersecurity competition today. The President's Cup brings together the nation's strongest cyber talent for a series of high-pressure, mission-driven challenges designed to test defensive skills, offensive tradecraft, and team-based strategy.

More than 800 individuals and 200 teams entered this year's President's Cup, which began in January with virtual qualifiers. Only the top federal cyber operatives advanced to the Finals, held in the Washington, DC area, which concluded the last week of May. Competitors were able to enter any or all of three tracks: Individuals Defensive Track, Individuals Offensive Track, or Teams, with each stage pushing their endurance, creativity, and technical expertise. Each mission simulated high-stakes cyber operations requiring precision, resilience, and deep technical knowledge.

The winners of the seventh annual President's Cup are (usernames are being used to protect individuals' operational security):

- **Defensive Track Champion:** "sheriffsparks," United States Navy
- **Offensive Track Champion:** "bdubya," United States Army
- **Teams Champion:** "ENOENTHUSIASM," United States Army & United States Marine Corps

"The President's Cup features the best cybersecurity talent the U.S. government has to offer," said CISA Acting Director Nick Andersen. "These champions rose above an elite field, securing victory through sharp analysis, decisive action, and advanced cyber tradecraft. We congratulate this year's winners and thank everyone who participated in the seventh annual President's Cup."

CISA leads and hosts the President's Cup each year to identify, challenge, and reward the best cyber talent across the federal workforce. The competition features high-impact cybersecurity scenarios — from responding to incidents and analyzing digital evidence to reverse engineering and hunting for threats — and it is open to federal civilian employees, as well as active duty and reserve military personnel.

Future participants can hone their skills and practice on earlier President's Cup challenges at <https://presidentcup.cisa.gov/>.

Thank you again for making the seventh annual competition Finals such a memorable event. "Literally half of the people in the individual finals were Army personnel and very likely 780th Military Brigade (Cyber) alumni and we had members on two of the five teams," said Robert Ighnat, OSE HHD

PC7 Teams, Finals

<https://presidentcup.cisa.gov/ctf/events/11>

1st Place: ENOENTHUSIASM: CPT Brian Welch, Army Reserve, former 780th/CSD (Cyber Solutions Development); MAJ Benjamin Allison, Army Cyber Institute, former 780th; CPT Jinny Yan, Army Reserve/USMA/EECS; Maj. Jason Russell, Marine Corps Forces Cyberspace Command (MARFORCYBER); MAJ Steve Rogacki, 781st MI Battalion (Cyber), 780th

5th Place: BitsOffTheRecord: MAJ Jason Decoursey, Operations Support Element (OSE), CSD, 780th; CPT Alexander Heldstab, OSE/CSD; CPT Aidan McCarthy, OSE/CSD; CPT John Eberling, former 11th Cyber Warfare Battalion developer, currently at 401st Cyber BN; and CPT Parabdha "Osho" Yonzon, 782d MI Battalion (Cyber), 780th

PC7 Defensive Track, Finals

<https://presidentcup.cisa.gov/ctf/events/9>

3rd Place: bdubya – CPT Brian Welch, Army Reserve

4th Place: helpme – CPT Yonzon, 782d MI BN

8th Place: Giftedflamingo – Mr. Ighnat, OSE/CSD

9th Place: Corp – SSG Robert Meyers, U.S. Cyber Command, recently left the service

10th Place: archang31 – LTC Michael Kranch, 780th MI BDE

PC7 Offensive Track, Finals

<https://presidentcup.cisa.gov/ctf/events/10>

1st Place: bdubya – CPT Welch

5th Place: archang31 – LTC Kranch

6th Place: Corp – SSG Meyers



U.S. ARMY

A Final Honor: *Inside the Fort Meade Military Funeral Honors Mission*

by Abigail Carey, Fort George G. Meade Public Affairs

FORT GEORGE G. MEADE, Md. — There is no room for error in military funeral honors. There are no second takes; every movement is a result of hours of deliberate practice. At Fort Meade, the Military Funeral Honors team treats every ceremony as the most important mission of the day, ensuring that every veteran receives the dignity and respect they earned.

The Fort Meade Military Funeral Honors teams are composed of all borrowed military manpower. These Soldiers from multiple units across the installation are trained for 30 days and serve on the teams for three months, traveling to funerals across a five-state region (Maryland, Washington, D.C., Virginia, Pennsylvania and Delaware).

Soldiers brought into the military funeral honors mission learn ceremonial marching movements, flag folding, uniform standards and how to perform the different varieties of funeral honors.

Each cycle of Soldiers performs approximately 200 funeral services during their three months serving with their teams.

Detail leader SGT Christopher Fisher of the 780th Military Intelligence Brigade (Cyber) said that military funeral honors is a mission that impacts him deeply.

“I take great pride in being able to honor the grieving families and give their loved one the most beautiful send-off that they rightfully deserve,” Fisher said. “But the nature of military funeral honors is a very somber mission, so it can take its toll on the

heart and soul.”

Being part of the military funeral honors mission made firing party member and bugler SPC William Jones understand the importance of military history.

“It’s one of those roles in the Army that make you understand that we are standing on the shoulders of giants,” Jones said. “Even though we’ve lost brothers and sisters, we keep going. And that’s beautiful.”

Former military funeral honors noncommissioned officer in charge, SSG Jarrett Turnipseed, said it is rewarding to give Soldiers the skills for this mission, but also to succeed in their careers.

“I’m training them to not only just do the mission, but I’m training them to think logistically, to plan and prepare, to function



U.S. Army soldiers practice flag folding ceremony during funeral honors training.

U.S. Army PFC Diaz calls out commands as soldiers, including PFC Munoz (left), practice flag folding procedures over a flag-draped casket during military funeral honors training outside a building on post. The soldiers, wearing Army Combat Uniforms with Operational Camouflage Pattern, are rehearsing the precise movements required for rendering proper burial honors to fallen service members. (U.S. Army photo by SPC Jesus Morales, 55th Signal Company (COMCAM).)

as a team and as individuals,” Turnipseed said.

He also said that being part of military funeral honors allows Soldiers to learn what service means.

“The Army is not just about boots on the ground in a combat zone and service is not just when bullets go flying,” Turnipseed said.

“Service is every day you put your uniform on and represent the United States Army and the sacrifices of those that have gone before.”

While the ceremony itself may only last a few minutes, the impression it leaves on the families remains for a lifetime. Through unwavering professionalism and deep

respect, the Fort Meade military funeral honors mission turns moments of immense grief into one of pride and remembrance. These Soldiers honor a legacy, ensuring that every veteran receives the dignity they earned through their years of service.



U.S. Army soldiers carry flag-draped casket during military funeral honors ceremony.

U.S. Army soldiers serve as pallbearers, carrying a flag-draped casket during a military funeral honors ceremony at an indoor chapel. The honor guard, wearing Army Combat Uniforms, carefully transport the silver casket adorned with an American flag through the chapel aisle. Soldiers identified by name tapes include Tran and O'Boyle. The solemn ceremony reflects the Army's commitment to rendering final honors to a fallen service member. (U.S. Army photo by SPC Jesus Morales, 55th Signal Company (COMCAM). ■



Honoring Our Fallen “*Lest We Forget*”

FORT GEORGE G. MEADE, Md. — The Fort Meade Military Funeral Honors team participated in the dignified arrival ceremony of PFC James Heigh. Killed in action in Italy during World War II, Heigh served with the 371st Infantry Regiment, 92nd Infantry Division.

Heigh's son, David Matthews, attended the ceremony along with Adjutant General of the Maryland National Guard MG Janeen Birkhead, Maryland Patriot Guard riders, an honor guard from the Department of Homeland Security and first responders. “It is our responsibility as citizens to remember the Nation’s brave fallen men and

women — whether they died on foreign lands in the heat of battle or after a lifetime in the uniform of our Army. Never forget the men and women who know all too much the cost of our freedom, for their service to this country is the greatest gift of all.”
—General John E. Hyten. ■





Praetorian Soldiers Represent Army Cyber



WHITE SANDS MISSILE RANGE, N.M. — Soldiers from the 780th Military Intelligence Brigade (Cyber) participated in the 37th Annual Bataan Memorial Death March, March 21, 2026, featuring a revised 15.6-mile route. The Praetorians placed 8th out of 23 registered teams in the Team Military Male Heavy category, with a time of 4:21:07.

The event honors U.S. and Filipino service members who defended the Philippines in 1942 during World War II. After surrendering to Japanese forces on April 9, 1942, the captured soldiers were forced to march for days—about 65 miles—through the Philippines' scorching jungles. Thousands died, and those who survived endured the hardships of prisoner-of-war camps and the brutality of their captors.

With roughly 5,000 participants joining in a high-desert march, the event was shortened due to high temperatures.

<https://bataanmemorialdeathmarch.itsyourrace.com/TeamList.aspx?id=6574>

780th Military Intelligence Brigade (5)

Peter Boyle

Luke Greys

David Kim

Robert Olander

Liam Schrader ■



Fort Meade Spring Fest



FORT GEORGE G. MEADE, Md. -- The 780th Military Intelligence Brigade (Cyber) was the only tenant military organization to support the annual Meade Spring Event hosted by the Meade Network of Schools at Meade High School on April 18.

The Praetorians engaged hundreds of participants; however, more importantly we met several attendees representing the Meade High JROTC program and the instructors responsible for Meade High's Homeland Security Signature Program. The instructors are starting a cybersecurity track in the fall and the Praetorian Soldiers and Civilians will assist with reviewing the curriculum and engaging the young people. ■





Sharing how the next generation can be all they can be

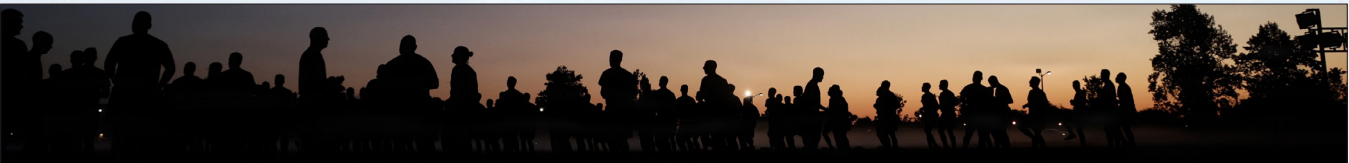
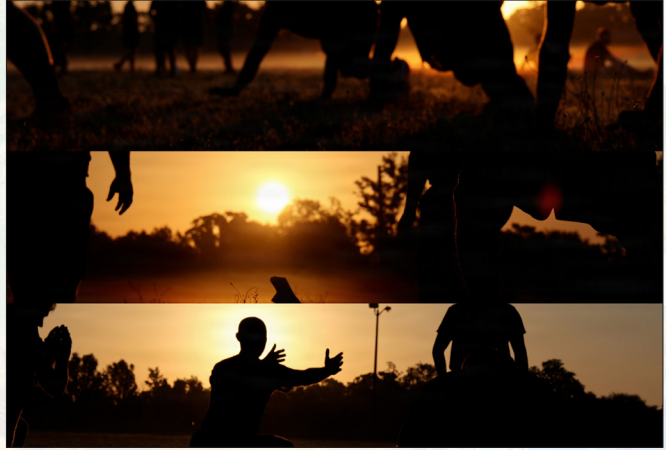


FORT GEORGE G. MEADE, Md. – 780th Military Intelligence Brigade (Cyber) and garrison Soldiers and Army Civilians attended a career day panel at Meade Middle School, May 26, as part of a series that gives young people an opportunity to learn more about different career fields.

This event focused on different opportunities within the military. Students learned about military life, the benefits of service and how the skills they use today connect to job fields within the military.

Thank you to Meade Middle School for this opportunity!
(courtesy photo) ■

NCOPD PT Session



FORT GORDON, Ga. -- Soldiers assigned to U.S. Army Cyber Command, conduct physical training during a Noncommissioned Officer Professional Development (NCOPD) session at Fort Gordon, Georgia, May 19, 2026. The NCOPD program is designed to develop and enhance the leadership skills, tactical proficiency, and professional knowledge of NCOs.
(U.S. Army photos by SSG. Matthew C. Garrett) ■

Joint Language Wars 2026

FORT GEORGE G. MEADE, Md. -- Cryptologic Warfare Group hosted the Joint Activity Language Wars event on May 11. The Joint Language Wars is a friendly competition between linguists across all service branches that tests their language competency through a variety of challenges. (U.S. Navy photos by Mass Communication Specialist 2nd Class Minh-Thy Plummer)



Aiden Che, language program coordinator at Marine Corps Support Battalion, left, and U.S. Army CPT Victor Kao, assigned to 780th Military Intelligence Brigade, review game rules before judging competitors in the Chinese portion of the 2026 Joint Language Wars on Fort George G. Meade, Maryland, May 11, 2026.



U.S. Army PFC Brandon Park, assigned to 780th Military Intelligence Brigade, left, and U.S. Air Force Tech. Sgt. Adrienne Saucedo, assigned to 22nd Intelligence Squadron, review game rules before judging competitors in the Korean portion of the 2026 Joint Language Wars on Fort George G. Meade, Maryland, May 11, 2026..



U.S. Army SFC Raj Chettri, assigned to 780th Military Intelligence Brigade, right, gives verbal instructions in Russian to U.S. Army PFC Andrew Jackling during a game at the 2026 Joint Language Wars on Fort George G. Meade, Maryland, May 11, 2026. ■





NEXT QUARTER'S BYTE IS focused on lethality and readiness for future combat. As in other issues of the BYTE magazine, the command encourages your contribution to drive the Cyber and Information Advantage conversation. If you have an article to share, write a synopsis and send it to steven.p.stover.civ@army.mil NLT August 14, 2026. Final articles are due August 31.

