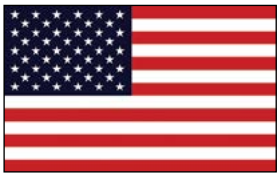

Army unveils new Army Biometric Program Directive

By Staff Sgt. Jacob Kohrs, Army News Service

As seen on TV, a crime scene investigator pulls a partial fingerprint off the shrapnel of a homemade explosive device and rushes it to his office. From there, it is handed off to the crime-lab examiner and scanned into the computer. Later, the fingerprint is matched to an individual, and the investigators head out to capture the perpetrator. In this scenario, the investigators use one type of biometric — a fingerprint — to identify a potential antagonist. The Army uses biometrics, measurable physical characteristics or personal behavioral traits used to identify a person, similarly but in a different manner.

Spc. Emily Lam, an internment resettlement specialist with the 357th Military Police Company runs a fingerprint scan on a prisoner utilizing the Biometrics Automated Toolset System, which recognizes insurgents and unwanted individuals in an area, as part of Pacific Warrior. Soldiers with the 11th Military Police Brigade spent two weeks in Fort Hunter Liggett, California training on basic Army Warrior Tasks, weapons qualification, military police specific tasks, and support tasks. Photo Credit: U.S. Army (Master Sgt. Andy Yoshimura).

The Army, as the executive agent for Department of Defense biometrics, leads the collection, storage and sharing of biometrics. They use biometric identification tools to help cut through disguises, such as name changes, hair color and gender alterations, to remove anonymity from a potential adversary.

In October 2022, the Secretary of the Army, Christine E. Wormuth, signed the U.S. Army Biometric Program, the first Army directive related to biometrics.

"The directive covers employment of Army biometric capabilities and operational actions," said Russell Wilson, the policy and engagements lead at the Defense Forensics and Biometrics Agency. "Operational actions from collection, matching, storing, sharing, analyzing, providing and, more importantly, deciding and acting. And it does that across the warfighter functions to facilitate lethal and non-lethal effects and complete Army missions."

The first DoD policy that dealt with biometrics came out in 2008. As the field grew, the need for a DoD Directive emerged and on Jan. 13, 2016, DoDD 8521.01E was approved as the DoD's official stance on operations for the employment of biometrics in military operations. It identified the Secretary of the Army as the DoD executive agent for DoD forensics and biometrics, which was then delegated to the Army's Office of the Provost Marshal General and further delegated to DFBA.

"[When DFBA] met with the Army Provost Marshal General's chief of staff, we identified a potential gap in the existing DoD directive for biometrics," said Wilson. "[Our] concern was with future or anticipated Army needs. We wanted to make sure that the Army was covered as we moved forward and make sure that we identified all the Army's needs throughout the warfighting continuum."

One of those concerns was the large number of authorities and policies the Army needed to deal with when trying to understand the guidance on the use of biometrics.

The operators or warfighters in the field collect identity information and send the data to a database that

Photo Credit: U.S. Army.

stores, matches and shares the enrollee's information. When this happens, privacy and civil liberties need to be considered and protected. Many DoD missions that utilize biometric technology take place overseas and need to be appropriately coordinated with foreign governments. As global affairs become more far-reaching, biometric collection for identification has expanded in force protection plans. Because of these trends, guidance for Army personnel must be clear and consolidated, and this directive codifies all U.S., DoD and Army biometric guidance, said Wilson.

As the Army moves forward with multidomain operations, identifying friend from foe — especially in an urban setting — becomes vitally important.

"[Biometric data] accurately identifies adversaries and enemies in real time, while verifying [them] from neutral identities with confidence," said Wilson. "And [it] helps the Army deny threat anonymity, which can prove critical in complex environments, like urban defense areas. It allows commanders to use the insights to better understand how to detect threat collusion."

Biometrics collected by the Army, and the rest of the military, are stored in the DoD's authoritative repository. The repository is interoperable with the biometric repositories of the FBI and the Department of Homeland Security. These systems working together provide U.S. forces with the information advantage needed to disrupt and deny a near-peer competitor, terrorist organization or individuals that intend harm, said Wilson.

Through this type of identity intelligence knowledge, a tactical level commander can have a better understanding of the operational environment. The sharing of biometric data contributes to an expanded understanding of adversaries – where they are from, location of last encounter, associated actions and enemy group affiliations.

Since May 2020, this directive has been thoroughly staffed throughout the Army to ensure it correctly identifies the processes that are needed for proper processing of information while ensuring privacy and civil liberties protections.

"We feel this is properly vetted," said Wilson. "It's been a lot of work ... but I think we've got it to a point where we're successful."

For a young Soldier, Wilson had one piece of advice when it comes to this Army directive and the use of biometrics.

"When you're out there doing your mission as a young Soldier, make sure you do it right, because these are people's lives, we're [dealing] with," said Wilson. "Obviously, we want to recognize that everybody is certainly endowed with inalienable rights, but we want to make sure that [these young Soldiers] understand that these services are there to help protect that Soldier on the ground. When it's done right, we'll be able to identify people who are definitely trying to do them harm, and the best thing we can do is make sure we do it properly." ■