More Effective DoD Encounter Management in Biometric & Identity Screening

By Nic Meyers

More Effective DoD Encounter Management in Biometric & Identity Screening

The DoD employs biometric collection and screening to enhance security at U.S.-controlled military installations around the world. Like all DoD biometric collection capabilities, they depend on the Automated Biometrics Identification System (ABIS) to process, store and report on collected biometric data acquired from foreign nationals requesting access to U.S. and allied installations overseas; and latent prints from improvised explosive devices and other hostile actions, enemy combatants and detainees.

In 2004, the Department of Defense (DoD) implemented a centralized biometric repository, the Automated Biometric Identification System (ABIS). This enabled the US Military to more efficiently track and identify threat actors in Operations Enduring Freedom and Iraqi Freedom. ABIS capabilities included the ability to store and process fingerprints, mug shots, iris scans and associated encounter and biographic information. It denied threat actors the anonymity that aliases and falsified documents formerly granted; you can’t lie about your biometrics.

These tools have proven enormously useful in identifying good vs bad actors around the world, and keep American servicemembers and civilians safe, but there remain significant gaps in the capability. An effective tool for mitigating these gaps is the concept of “Encounter Management.” Encounter Management is a derivative set of processes and standards that dictate the actions security personnel or biometric collectors should take during an encounter or collection event. This includes the appropriate response to be taken when a Significant Activity (SIGACT) occurs or a threat actor is identified.

While biometrics are veritable, they only represent one aspect of an identity.
Encounter Management at the Operator Level

Applicable policies and directives change as rapidly as the supporting science and technology. Unfortunately, ground-level operational guidance takes additional time to trickle down. Tactical Encounter Management policy is often outdated, or not thoroughly constructed, which impacts the ability of biometric screeners to make informed decisions during a biometric/identity encounter, potentially putting the safety of US Service Members and facilities at risk.

Where resources are limited, identity screening operations are sometimes supported by personnel lacking the expertise or suitable training, or, in extreme cases, a military operation has appointed personnel from unrelated fields—such as truck drivers or information technology specialists. In the absence of applicable or accessible policies, operators may unwittingly pursue unsafe courses of action when encountering threat actors. Errors in decision-making are inevitable if security personnel are not provided detailed policy and procedures. This is most problematic in austere environments with an active security threat, such as Horn of Africa or Iraq, where effective Encounter Management is critical. Effective Encounter Management requires a layered approach to incorporate local, organizational, and strategic guidance. A comprehensive policy will:

- Ensure the safety of personnel
- Adequately inform all parties of the identity, disposition, and possible threat of an individual
- Utilize the DoD Biometrically-Enabled Watchlist to enhance screening processes

In a post-OIF environment, where kinetic operations are less common, and many soldiers lack the experience of managing a security mission in high-threat environments, the onus is on their leadership and theater “owner” to establish that encounter management process and ensure it is integrated into security policies.

Identity Intelligence (I2) Is Key to Effective Encounter Management Policy

A common misconception among security personnel or biometric screeners is the assumption that biometric screening sufficiently ascertains a subject’s identity and disposition. While biometrics are veritable, they only represent one aspect of an identity. Take for instance, the following example:

Subject A crosses a checkpoint with what is believed to be his family. His biometrics and biographic data are captured and submitted for screening. The resulting report states the subject was administratively encountered in 2016 during a routine patrol, but nothing derogatory was noted at that time. If additional “identity intelligence” (I2) analysis was conducted against the subject, they would discover national level reporting published by the Defense Intelligence Agency (DIA) that consistently places Subject A as an improvised explosive device (IED) builder from a neighboring province. In this case, that person could have been detained until further investigation could be accomplished.

A “whole of person” approach should be taken when evaluating a subject’s threat level and can be accomplished by conducting additional identity analysis, based on gathered intelligence such as documents and media, in parallel to biometric screening. This type of analysis is referred to as Identity Intelligence (I2). In addition to biometric screening, identities need to be analyzed by I2 trained personnel. Other reporting can link the subject to nefarious activity; such data includes biographic information, “soft biometrics” like hair color or tattoos, affiliations, or other miscellaneous data like passports or phone numbers.
Biometric screening by itself results in one of three general categories of biometric match response:

- No-match – no previous biometric encounter; however, additional identity analysis should still be conducted.
- Administrative match – usually indicates a standard encounter in theater or former employment, but no derogatory encounters.
- Watchlist match – the subject’s biometric data is associated with a watchlist record.

Encounter Management policies will outline the process for addressing various response categories. For example, the operator will react differently to a subject who matches within a non-violent category (such as theft) versus a subject who poses a high threat to personnel. These policies should be driven top-down and provide clear guidance on conducting biometric screening and I2 from the strategic level to the operator level.

**Enabling Technologies Can Enhance Screening**

Identity management solutions such as the Near Real-Time Identity Operations (NRTIO) Regional Forward Server (RFS) are increasingly used to provide enhanced biometric screening capabilities to force protection missions in theater. The NRTIO RFS provides a regionally located, authoritative subset of the national dataset for biometric screening. Being regionally aligned, it provides a quicker response time, direct to the collector’s device, and allows them more opportunity to respond to their encounter.

Effective employment of a tool like NRTIO can mitigate many of the risks outlined above. The application provides a centralized solution for transmitting, reporting and disseminating biometric data. Implementing such an architecture into security missions enhances each facet or tier of screening by delivering an established identity operations architecture.

**A Four-Tiered Approach to Screening**

**Operator Layer**

At the ground level, the collector requires detailed guidance on supporting Encounter Management and Force Protection operations. This needs to be specific and provide an action roadmap for all scenarios that could be encountered in the enrollment process. This guidance can be derivative of higher headquarters policies but must be tailored to meet local mission needs. Ideally, input will be provided by security and intelligence personnel/teams; and identity activities. While the biometric collection device transmits enrollments to authoritative US Government systems for screening, it should also contain a subset of threat actors in the onboard watchlist. This list can be tailored and provides an immediate response, whereas the larger enterprise will take up to three minutes. The list should contain threat actors with a nexus to that region or locality.

**The Communications Layer**

Stepping through the screening process, the next step is the communications layer. This is the least discussed and most critical tier. Without an ability to transmit data to more robust, authoritative US Government systems, collectors are severely constrained by the small number of watchlist records stored on their device that they can match against; or they encounter the network lag associated with common communication methods, such as NIPR or SIPR transmittal using email or other tools. In both cases there are additional risks to consider if a response is not readily available. Successful architectures like the NRTIO or SOCOM’s SOFEX employ intermediate communication platforms, such as 4G routers or tactical satellite communications.
**Authoritative Screening Layer**

After the communication system transmits the collection, it arrives at authoritative systems. These include regionally located datasets, and those stored within the Departments of Defense, Justice and Homeland Security. Collectively these provide the opportunity to match against a significantly larger pool of data than could ever be stored locally onboard the collection device. Using the NRTIO architecture, they also ensure a response is provided within three minutes, informing the collector’s actions with minimal lag time.

**The Final Tier**

The final tier that supports this process is the national and strategic level assets, that include organizations specializing in Identity Intelligence (I2), Watchlist Management, Force Protection (FP) operations or counter intelligence (CI). Collectively these organizations provide input to the watchlist data, identifying threat actors, publish analytical reporting and provide the much-needed context on a subject to paint a picture of the person behind the biometric. This information is critical in guiding the ground level collector in their decision making. Even if a subject is not immediately identified as a threat due to their biometric not being associated with the biometrically-enabled watchlist, it does provide the opportunity to link biometric encounters with new intelligence as it becomes available.

**Conclusion**

An effective Encounter Management program should incorporate biometric collection and screening, and Identity Intelligence (I2) analysis. A well laid out Encounter Management process describes the actions taken at the point of encounter, guides the handling of a subject during the enrollment and screening process, and specifies courses of action to be taken once an identity is verified.

Additionally, screeners and security personnel will benefit from a deeper knowledge of institutional policies on identity and encounter management, and how to incorporate it into their security and force protection operations. This allows them to take a proactive approach in maintaining and enhancing their screening processes and security readiness.

Nic Meyers is the Deputy Program Manager for Near Real Time Identity Operations (NRTIO) at Envistacom, LLC.