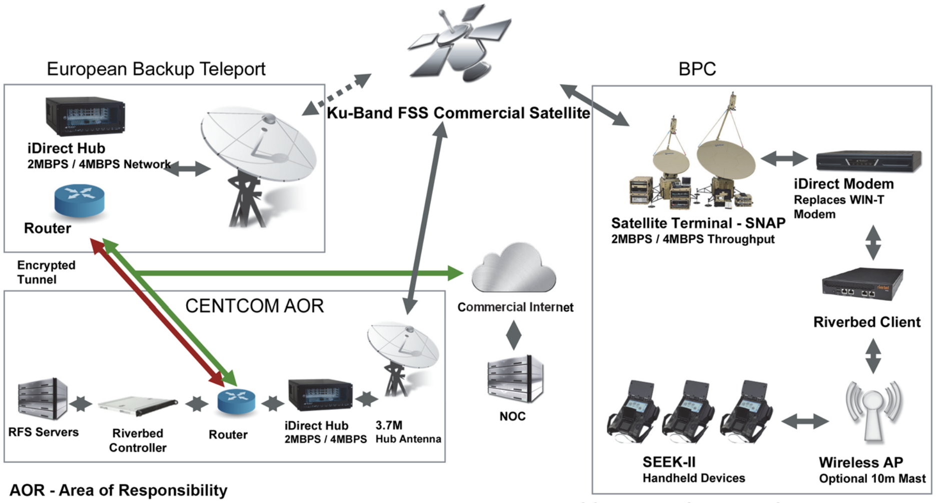
Near Real Time Identity Operations (NRTIO)

Executive Summary

- Near Real Time Identity Operations (NRTIO) is a Joint Emerging Operational Need (JEON) intended to provide the following capabilities to U.S. Central Command (USCENTCOM) in support of Operation Inherent Resolve:
  - Near real-time identity information to U.S. conventional forces to enhance force protection, stem the flow of foreign fighters, and counter the threat from IEDs
  - Increased partnership capacity by sharing collected biometric data with partner nations and other coalition forces to establish the identity of adversaries transiting the USCENTCOM Area of Responsibility (AOR)
- NRTIO achieved Initial Operating Capability (IOC) in February 2016, and the Army Test and Evaluation Command (ATEC) conducted an IOC operational assessment (OA) from March through July 2016 using data from the USCENTCOM AOR.
- Test limitations precluded the assessment of operational effectiveness, operational suitability, and cybersecurity during the IOC OA, including:
  - Due to the IOC state of NRTIO, soldiers could not use its full capability. The biometric dataset on the Remote Forward Server (RFS) was incomplete, which reduced the rate of biometric submission matches against the biometrically enabled watchlist (BEWL). The IOC OA demonstrated that biometric submissions to the RFS had a lower than acceptable match accuracy.
  - To avoid disruption to real-world missions, USCENTCOM did not permit testers in theater but ATEC received 25 survey responses from NRTIO users. It is not known if these responses represent a statistically significant sample size.
  - USCENTCOM did not permit cybersecurity testing on the production hardware and software due to mission constraints.
- During the IOC OA, soldiers successfully completed enrollments and matches with their local collection device against watchlists on the NRTIO RFS and the DOD authoritative database (Automated Biometric Identification System (ABIS)). Due to IOC OA constraints, RFS response timeliness could not be adequately assessed. During the OA, most biometric submissions consisted of batch submissions of biometric enrollment records, which are not near real-time submissions. As part of the OA, the capability to make biometric submissions and receive near real-time responses was demonstrated but the sample size is not statistically significant.



AOR - Area of Responsibility
AP - Access Point
BPC - Building Partnership Capacity
CENTCOM - Central Command
FSS - Fixed Satellite Service
MBPs - Megabits per second

NOC - Network Operations Center
RFS - Regional Forward Server
SEEK-II - Secure Electronic Enrollment Kit
SNAP - SIPRNET/NIPRET Access Point
WIN-T - Warfighter Information Network-Tactical

- Prior to reaching Full Operating Capability (FOC), NRTIO requires a technical modernization to improve the accuracy and completeness of the RFS biometric dataset. An accurate and complete biometric dataset in the RFS that contains all of the watchlisted identities relevant to the USCENTCOM AOR is necessary to demonstrate near real-time identity operations.

System

The NRTIO JEON intends to provide the forward-deployed Service member the capability to receive an identity response in near real-time of submission of biometric information. The IOC OA configuration includes:

- Handheld Biometric Collection devices. The Secure Electronic Enrollment Kit (SEEK) II performs fingerprint capture, dual iris scan, and facial capture. The devices are compliant with Electronic Biometric Transmission Specification (EBTS) and Electronic Fingerprint Transmission Specification (EFTS), which are requirements for interface with ABIS.
- Dedicated communications capacity including tactical satellite (TACSAT), satellite communications (SATCOM), and WiFi connectivity.
- RFS. The RFS includes the USCENTCOM AOR-specific biometric records that allow for rapid, non-authoritative match results to be provided to the forward deployed warfighter. ABIS verifies the biometric matches using the authoritative database, which possesses a larger dataset.
- Web-based Exploitation and Analysis Portal. An identity operations portal that provides web-based real-time collaboration, automated report generation, materiel management, data search and correlation, alerting, and a database for exploitation and collaboration. The portal used

during the IOC OA was the Identity Resolution Exploitation and Management Services Collaborative Workstation (ICW).

Mission

- USCENTCOM forces use the NRTIO IOC capability for identity operations to provide timely, accurate, and complete responses indicating whether persons of interest encountered in the field have a prior history of derogatory (e.g. criminal) activity, to assist in identifying potential threats to U.S. forces and facilities throughout the USCENTCOM AOR.
- Upon achieving FOC, forward-deployed Service members will use NRTIO to provide biometric responses including tailored biometric matching and watchlisting within the USCENTCOM AOR.

Major Contractors

- Booz Allen Hamilton – Belcamp, Maryland
- Envistacomm LLC – Atlanta, Georgia

Activity

ATEC conducted the following testing in FY16:

- The IOC OA of the NRTIO system from March to July 2016
- A cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) during developmental testing of a clone of the IOC portal, one component of the NRTIO, in July 2016

Assessment

- The IOC OA leveraged the operational assessment process of the JEON and focused on whether the technology is viable to meet the warfighter requirements and will be used to inform the tailored Test and Evaluation Master Plan (TEMP) and operational test plan to support FOC. At the FOC OA, the operational assessment will focus on the operational effectiveness, suitability, and survivability of the NRTIO system under test. Accordingly, the test needs to have a DOT&E-approved test plan and tailored TEMP.
- During the IOC OA, the biometric dataset on the RFS was incomplete, which reduced the rate of biometric submission matches against the BEWL. To meet mission timelines, ATEC started operations on the RFS without the complete biometric and latent dataset relevant to the USCENTCOM AOR. Match consistency between the RFS and ABIS is a key criterion for establishing operator confidence in the RFS. If biometric matches are missed by the RFS, a potential person of interest may not be identified. The RFS technology limitation of having not fully ingested the entire biometric database precluded assessment of the dynamic synchronization of the DOD BEWL with the RFS.
- Due to IOC OA constraints, DOT&E could not adequately assess RFS response timeliness. During the OA, most biometric submissions consisted of batch submissions of biometric enrollment records, which are not near real-time submissions. As part of the OA, the capability to make biometric submissions and receive near real-time responses was demonstrated. However, the majority of the IOC OA biometric enrollments were submitted using a bulk file upload to the portal, which forwarded the data on to both ABIS and the RFS. Bulk uploading of biometric submissions is adequate for many operational needs.
- To avoid disruption to real-world missions, USCENTCOM did not permit testers in theater but ATEC received 25 survey responses from NRTIO users. It is not known if these responses represent a statistically significant sample size. Survey responses noted suitability problems that included high workloads including periods of enrollment surges, long upload times, and communications outages. There were many non-materiel shortcomings. Areas to address to improve suitability include lack of leadership awareness of the importance of biometrics, the need for intensive training of soldiers with no prior biometrics experience, and transportability hardships because of the hostile terrain in parts of the USCENTCOM AOR.
- ABIS operators at the Biometrics Identity Management Agency reviewed over 800 NRTIO biometric enrollments to assess whether soldiers were able to collect biometric data of match quality. For the NRTIO biometric enrollments, fingerprint quality was generally acceptable for obtaining accurate matches, whereas iris and facial images showed greater variability. Since most matches primarily rely on fingerprint data, the data quality of NRTIO biometric enrollments was adequate to support identity operations.
- Mission constraints prevented an adequate assessment of the cybersecurity posture during the ATEC-conducted CVPA on a clone of the ICW.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The Army should:
  1. Mature tactics, techniques, and procedures and address manpower requirements to improve suitability prior to FOC.
  2. Prior to FOC operational testing, load the current USCENTCOM subset of the BEWL on their SEEK IIs, so watchlisted individuals can be identified in near real-time.
  3. For FOC, streamline or automate training to improve the suitability of NRTIO.
  4. Conduct an operational CVPA and Adversarial Assessment on the NRTIO system including the RFS prior to FOC.
  5. Complete a technical modernization of the NRTIO system that has an accurate and complete biometric dataset in the RFS that contains all of the watchlisted identities relevant to the USCENTCOM AOR prior to FOC.
  6. Provide an operational test plan and tailored TEMP 30 days prior to the start of the FOC OA to DOT&E for approval.