OBJECTIVE: Research and develop a federated identity management software system that leverages techniques to match encrypted biometrics (such as fingerprint, face, iris, Deoxyribonucleic Acid (DNA), etc.) data and utilize multiple techniques that encompass biometric template protection. The work will leverage a feature transformation and multi-biometric cryptosystems utilizing secure biometric schemes to create derived biometric templates. This approach will create revocability/renewability and un-linkable identification information that is not directly traced back to the original biometrics, thus increasing data security.

DESCRIPTION: The integrated biometric capabilities across the Joint, Interagency, International, Multinational (JIIM) communities greatly increase overall Identity Activity mission readiness in Biometric Enabled Intelligence (BEI) analysis, in support of theater operations with mission enablers for force protection, intelligence, physical and logical access control, identity management/credentialing, and interception operations. Therefore, there are urgent needs, such as maintaining confidence and strengthening our relationships with international communities by demonstrating a wider array of biometric protection capabilities to partner nations. The overall security of this development will minimize or prevent access to biometric data. In the enrollment stage, biometric data is stored as a reference template in a standard format. The biometric data of the person of interest is transformed (or rather derived) into a candidate biometric template for matching against the reference template and cross-matching templates from different databases. The derived biometric template is designed to reveal little or no information about the original biometrics of an individual. The derived biometric template from the original template should conform to the requirements of irreversibility, revocability/renewability, and un-link-ability. "Irreversibility" emphasizes that it is impossible to generate the original template from a person’s derived biometric template. "Revocability/Renewability" implies the ability of revoking and re-issuing the derived biometric template. "Un-link-ability" prohibits the trace of the multiple derived biometric templates to the same original template. The optimal solution is the federated biometric software system with novel techniques to identify/verify invaluable and irreplaceable identity information within an enterprise environment. To maximize protection, the proposed federated software systems should be able to run application software tools at various local storage of derived biometric templates that use encrypted protection schemes/mechanisms in the multi-biometric cryptosystems.

PHASE I: Research and list various types of technologies associated with the proposed approach to develop a prototype software and a technical report that has the following considerations: 1) leveraging existing technologies and upcoming technical advances that address the technical challenges; 2) provide a detailed description of the problem areas and the associated solutions with full explanation of the proposed disciplines, procedures, techniques, capabilities, and resources; 3) describe the operational constraints, feasibility of each approach, capability, applicability, assumption, and restrictions of the outcomes of the proposed effort; 4) indicate which software architecture and development environment (software tools, interface requirements, specifications of input/output data, etc.) would work optimally in a Windows (laptop and desktop) environment; and 5) list the methods and criteria for the performance measurements. Deliver a technical report on the study findings, algorithms, models, techniques, and software architecture of the proposed software system for the next phase development along with the implementation and evaluation plan of the proposed capabilities.

PHASE II: Research and develop a prototype software and technical report that captures the following focus areas: 1) encrypted-derived biometric templates; 2) multi-biometric cryptosystems; 3) processes of encrypted biometric data via application tools at the local storage level for identification and verification of people of interest; 4) enhancement of models of running multiple application tools at various local databases; and 5) development of scientifically sound methods (metrics, experiments, etc.) to evaluate the overall capability of the software. The technical report shall list the strengths and limitations of all algorithms, software models and techniques, and proposed architectures that were explored.

PHASE III DUAL-USE APPLICATIONS: The techniques and algorithms developed in this effort may be leveraged in a broad range of potentially high payoff military and civilian applications. The prototype system will increase the protection of data and enhance the identification of people of interest. The focus is to transition the development into U.S. Army Programs of Record that support the commander’s decision and increase situational awareness. In addition to supporting not only military and other government agencies to identify, track, and reunite civilian populations during Security, Stability, Transition, and Reconstruction (SSTR) and Humanitarian and Disaster Relief (HADR) efforts. Law enforcement agencies and private companies will have the capability to enhance their security
and protect Personally Identifiable Information (PII) data.

REFERENCES:
1. medium.com/syncedreview/federated-learning-the-future-of-distributed-machine-learning-eec95242d897
2. researchgate.net/publication/278671027_Identification_Using_Encrypted_Biometrics
3. pdfs.semanticscholar.org/83de/c5bff60692964a140180e71e6775ab54991e.pdf

KEYWORDS: Federated identity management, irreversibility, revocability/renewability, and un-link-ability