Person-Centric Identity Management

Rapidly Assimilating Data About a Person of Interest

Recent terrorist attacks in the United States and around the world clearly illustrate the need for the rapid assimilation of data surrounding the perpetrators, both to verify and confirm the identities of perpetrators as well as potentially to expand the actionable identity-related intelligence required to prevent follow-on attacks or terrorist activity.

A Case for Action

The U.S. government screens millions of travelers, workers (who may be seeking employment with access to critical infrastructure, information, and transportation systems), refugees, and individuals visiting or immigrating to the United States and its territories. The vast majority of the data collected is stored in stand-alone and stovepiped systems with limited or no data sharing capabilities, no standard correlation capability to resolve and link identities, and no substantive capability to link additional peripheral encounter data (e.g., information gleaned from social media, checkpoint screening results, or other relevant agency records).

The U.S. government needs a robust Person-Centric Identity Management (PCIM) capability. PCIM enables the resolution and aggregation of multiple un-linked identity records (and associated data) to form a singular, comprehensive, and high-confidence view of an individual (subject to the appropriate security, privacy, and civil right/civil liberty legal protections).

Understanding the Problem

Currently, the U.S. government lacks an overarching PCIM capability, which results in:

- An inability to rapidly federate and share person-centric data, necessary to respond in near real time to acts of terrorism and law enforcement activities.
- Insufficient immigration data integration, necessary to allow officials to seamlessly track individuals through the enforcement and benefits systems.
- A diminished intelligence analytical capability, necessary to proactively resolve established identities (linked to encounter data) in order to provide actionable intelligence before and after events occur.

> **"There were so many mistakes made...I wouldn't pick out the [Commonwealth] Fusion Center but obviously we need to review this whole situation...How did he [Tamerlan Tsarnaev, one of the Boston Marathon bombers] get out of the country with only the DHS knowing? They didn't know when he came back. The FBI dropped him from the list, the whole lack of coordination and information ...clearly a lack of coordination among agencies"**
>
> –SENATOR JOHN MCCAIN,
> QUOTED IN "DATA-SHARING TROUBLES RAISE QUESTIONS IN MARATHON CASE," BOSTON GLOBE, APRIL 2013

MITRE

The MITRE Corporation is a not-for-profit organization chartered to work in the public interest. We apply our skills in systems engineering, research and development, and information technology to help the government address issues of critical national importance.

- A limited ability to share "best of breed" screening and vetting solutions across federal agencies (and with state and local authorities), thus diminishing the quality of personnel vetting, checkpoint screening operations, and counterterrorism at all levels of government.

Areas of Opportunity

The Secretary for the Department of Homeland Security should consider establishing a department-level, cross-government initiative to create a PCIM capability. A robust PCIM capability will provide a federated view of all the identities that an individual has established across the federal landscape (and ultimately with state and local authorities) that will link all privileges, benefits, accesses, and credentials that the individual may possess. This overarching person-centric identity is linked to the biometric and biographical records, identity assurance levels, agency records, and encounter data that constitute a "complete" view of the individual's interaction with various government entities.

PCIM will provide an overarching, holistic view of an individual, improving:

- **Terrorism Response:** Accelerating to near real time a query capability across all data stores to enhance counterterrorism and law enforcement response times.
- **Refugee Vetting:** Strengthening the process by automating the flow of person-centric information and vetting results among DHS, DoD, DOJ, DOS, and the various intelligence community partners.
- **Immigration Enforcement:** Allowing DHS to link immigration data across the department to facilitate stakeholder access to real-time data in support of immigration processing (benefits and enforcement), trend analyses, and border security.
- **Border and Checkpoint Security:** Allowing federal, state, and local agencies to link person-centric data to critical infrastructure screening operations—airport checkpoints, entry/exit locations, and other critical infrastructure checkpoints/screening technologies.
- **Vetting Shared Services and a Common Approach to National Counterterrorism Center (NCTC) Vetting:** Strengthening identity resolution, shared vetting services, and a standard approach to NCTC vetting.
- **Person-Centric Analytics:** Laying the groundwork for actionable predictive and prescriptive analytics in order to provide advanced warnings and indicators to prevent acts of terrorism before they occur.

For further ideas about applying the guidance in this paper to your agency's particular needs, contact federaltransition@mitre.org.