

Our National Urgency to ‘Connect all the Dots’™ with deep Information Sharing

In the aftermath of 9/11 and recent terrorist attacks, it is clear that US intelligence and law enforcement agencies still lack the most meaningful, relevant, and timely *global knowledge fusion*™ to prevent attacks. The recent assessment of the December 25 incident by the *Senate Select Committee on Intelligence* confirms that the government continues to lack the technical ability to conduct real-time analysis with instant alerts *-simultaneously across* the massive numbers of isolated datasets held by different government entities so as to *discover* threads and associations and ‘connect all the dots’™ among them in time to interdict. Past and current programs have at best connected *some* of the dots by reproducing even larger centralized collections but fail to incorporate new technology architectures which can simultaneously connect enough dots so as to consistently reveal the correct picture at the right time.

Most attacks within the US by terrorists have been conducted by persons entering the country through our ports. The FBI Director predicts that terrorists as well as weapons of mass destruction will enter the US legally and illegally. In order to interdict attacks, there is an urgent need for deep information sharing with instant alerts *simultaneously across* increasingly larger sets of distributed databases –all generated, received, and maintained moment-to-moment by the Dept. of Homeland Security plus many other IC and non IC sources. Disconnected but critically related knowledge nuggets buried among the combination of *all* these sources is critical if we are to expose terrorist threats crossing US borders and entering US ports.

One of the ways that DHS is currently addressing its part of the larger and more pervasive, government-wide ‘stovepipe’ problem is through a joint initiative of the Office of Intelligence and Analysis (OI&A) and US Customs and Border Protection (CBP). OI&A is responsible for using information and intelligence from multiple sources to identify and assess current and future threats while CBP is responsible for preventing terrorists and terrorist weapons from entering the US. The joint initiative is called *Enterprise Cross Domain Services* (ECDS), which utilizes advanced, patented information fusion technology in ways heretofore impossible. This technology has been developed over a decade as a public/private effort with the collective participation of Universities, DARPA, CIA, NSA, FBI, the Navy, the Air Force, NCTC, NCIS, DHS, and other agencies.

ECDS has already created a massively scalable *distributed* analysis capability indexing across nine billion records from 25 different CBP databases – pedestrians, automobiles, trucks, ships, and cargo entering the US daily. Most indexes are updated daily. Flight manifests are processed in real-time. Indexes will also include historic and real-time data which reside within applications of the Container Security Initiative, the Secure Freight Initiative, the Domestic Radiation Detection initiative, the Office of Operations Coordination, the Domestic Nuclear Detection Office, the Automatic Message Handling System (AMHS), and the Transportation Security

Administration (TSA), and Immigration and Customs Enforcement (ICE). ECDS is building an ability to *connect the dots* across DHS distributed organizations, applications, and datasets, without disrupting current operations. This system can also serve as a ‘contextual’ value –added complement to the rules-based Automated Targeting System (ATS), and can seamlessly interface with FBI, State Department, NCTC, as well as any other counterterrorism data sets. This is a potential *game-changing* model for government-wide counterterrorism discovery and alerting across multiple agency data sets in real time. However, *deploying* this proven capability requires multi agency cooperation, executive support, and additional funding.

The patented technology being utilized by ECDS is the same technology that was successfully deployed in a DNI sponsored multi- agency IC information sharing pilot then known as IS-FAST, and field proven with praise from FBI and the Treasury Department in Congressional testimony. It is in use today by 8,000 Joint Terrorism Task Force (JTTF) analysts and agents in the FBI’s Investigative Data Warehouse, the use of which helped earn the only ‘A’ score in the ‘counterterrorism report card’ issued by the members of the *9/11 Commission*. This technology adheres to related published recommendations and requirements articulated by *Markle Foundation’s Task Force on National Security in the Information Age*, DNI; Congress.

With appropriate management endorsement, the DHS ECDS system can demonstrate within 90 days the ability for a Joint Terrorist Task Force Analyst to run a query/analysis session across 10 billion items in multiple databases indexed by DHS ECDS and the FBI IDW, including the State Department’s Consolidated Consular Database (CCD), the Terrorist Screening Center (TSC) ‘watch list,’ and the TSA ‘no-fly list’ – providing parallel processing for cross-agency real-time terrorist threat detection and assessment over secure networks. In the second 90-day spiral, the operational pilot will be made available for use and evaluation by 50 trusted and cleared FBI, NCTC, and other JTTF analysts, with user accountability and audit capability. Within the third 90-day spiral, an interface to the system will be made available to FBI, NCTC, and other counterterrorism applications. The fourth 90-day spiral will expand the number of data sets and increase multi-agency analysts and agent users to at least 10,000.

The cost to deploy this proven, low risk, low cost operational pilot would be minimal. All the data would continue to be securely held by the agencies that collect and protect it today, without copying, consolidating, or moving it. Secure classified networks enable the indexes to communicate with each other in parallel without interference to existing operational systems or other applications. Funds will provide additional indexing, analysis, and alerting capacity, integrate more data sets, and provide rapid roll out with training for NCTC, FBI, DHS OIA, and other counterterrorism analysts. A report to Congress 180 days into the project will verify accountability and auditable compliance with privacy laws prior to a broader deployment.