Integrated Suspicious Activity Reporting and Decision Analysis System (iSARs)
October 2012 to September 2013

Michael Orosz
Information Sciences Institute (ISI)
mdorosz@isi.edu

“This research was supported by the United States Department of Homeland Security through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under Cooperative Agreement No. 2010-ST-061-RE0001. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security or the University of Southern California.”

Cooperative Agreement No. 2010-ST-061-RE0001
Department of Homeland Security

December 31, 2013
ABOUT CREATE

Now in its tenth year of operation, the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) was the first university-based Center of Excellence (COE) funded by University Programs of the Science and Technology (S&T) Directorate of the Department of Homeland Security (DHS). CREATE started operations in March of 2004 and has since been joined by additional DHS centers. Like other COEs, CREATE contributes university-based research to make the Nation safer by taking a longer-term view of scientific innovations and breakthroughs and by developing the future intellectual leaders in homeland security.

CREATE's mission is to improve our Nation's security through research and development of advanced models and tools to evaluate risks, costs and consequences of terrorism and natural and man-made hazards and to guide economically viable investments in homeland security. We are accomplishing our mission through an integrated program of research, education and outreach that is designed to inform and support decisions faced by elected officials and governmental employees at the national, state, and local levels. We are also working with private industry, both to leverage the investments being made by the Department of Homeland Security in these organizations, and to facilitate the transition of research toward meeting the security needs of our nation.

CREATE employs an interdisciplinary approach merging engineers, economists, decision scientists, and system modelers in a program that integrates research, education and outreach. This approach encourages creative discovery by employing the intellectual power of the American university system to solve some of the country’s most pressing problems. The Center is the lead institution where researchers from around the country come to assist in the national effort to improve homeland security through analysis and modeling of threats. The Center treats the subject of homeland security with the urgency that it deserves, with one of its key goals being producing rapid results, leveraging existing resources so that benefits accrue to our nation as quickly as possible.

By the nature of the research in risk, economics, and operations, CREATE serves the need of many agencies at the DHS, including the Transportation Security Administration, Customs and Border Protection, Immigration and Customs Enforcement, FEMA and the US Coast Guard. In addition, CREATE has developed relationships with clients in the Offices of National Protection and Programs, Intelligence and Analysis, the Domestic Nuclear Detection Office and many State and Local government agencies. CREATE faculty and students take both the long-term view of how to reduce terrorism risk through fundamental research, and the near-term view of improving the cost-effectiveness of counter-terrorism policies and investments through applied research.

In 2011, the University of Southern California (USC) and a team of 23 partner institutions were awarded a new 5-year Cooperative Agreement resulting from a recompetition of the Center’s charter. This annual report covers the third year under Cooperative Agreement 2010-ST-061-RE0001, the ninth year overall of CREATE’s DHS funding, from October 2012 to September 2013.
1. Executive Summary ................................. 3
   1.1. Project Overview .................................. 3
   1.2. Project Status/Accomplishments .................. 4
2. Research Accomplishments ........................... 5
   2.1. Research Products ................................ 5
   3. Research Transition ................................. 6
   3.1. Applied Relevance ................................ 6
   3.2. Collaborative Projects ............................ 6
3. Education ........................................... 6
4. Outreach ............................................. 7

1. Executive Summary

   1.1. Project Overview

An important element in preventing terrorist attacks are suspicious activity reports (SARs) filed by citizens and local law enforcement. Intelligence analysts review incoming SARs, query various government databases and intelligence sources, and establish patterns and relationships. SARs that are deemed to be terrorism-related are ultimately passed along to other intelligence consumers (e.g., the FBI), who assess its actionability and decide on follow-up action (e.g., conducting surveillance, defensive action).

At present, much SARs tasking and analysis is accomplished manually, using many qualitative and judgment-based risk and decision processes. This leaves open the possibility that key events and connections may be overlooked – with potentially catastrophic consequences. The Integrated Suspicious Activity Report and Decision Analysis System (iSARs) project is based on the assumption that the defender can better detect, predict, and prevent attacks, based on:

- collected evidence (i.e., past SARs)
- historical evidence (i.e., previous events)
- potential capabilities of adversaries and resources available to them
- potential attack targets within their Area of Responsibility (AOR)
- the experience and intuition of the intelligence analysts

The project will develop tools, methods, and processes for enhancing the risk-driven intelligence collection, analysis, and decision-making capabilities of the U.S. domestic law enforcement and intelligence community. This will be done by combining SARs and other intelligence products with risk and decision analysis techniques to help better detect possible adversarial plans and assess the threats that are associated with the greatest probability of occurrence.

Based on discussions by the research team with intelligence professionals at the Joint Regional Intelligence Center (JRIC) fusion center in Los Angeles, CA, and the Orange County Intelligence Assessment Center (OCIAC) fusion center in Orange, CA, the primary project thrusts (which overlap somewhat) are:

1. greater tagging/categorization of SARs (beyond just the eight ‘pre-incident indicators’ of terrorism);
2. defining more clearly the threshold for what constitutes a meaningful SAR;
3. assessing the value of having acted upon SARs that were passed up the chain (i.e., to the FBI), but from which nothing ultimately came (the ‘intel black hole’);
4. devise a standardized way of measuring progress, successes, or failure of the overall SAR system – beyond the level of an individual SAR.
A key aspect of working this problem will be acquiring data – related to past SARs and, ideally, also the particular outcomes that resulted from them (e.g., surveillance, arrests, disruption of plots, subsequent investigations). Much of this information space is classified or otherwise sensitive, making collection of SARs challenging. To overcome this, a three-pronged data acquisition approach will be taken:

1. work with DHS to access the National SARs Database (which contains sensitive but not classified SARS);
2. work with the JRIC and OCIAC fusion centers to access past SARs they have processed;
3. work with local law enforcement and other first responder agencies (from which the majority of SARs originate) to access past SARs processed by these agencies.

Additionally, in close consultation with OCIAC and JRIC, local law enforcement agencies, and others knowledgeable of intelligence analysis and suspicious activity detection, a series of fictitious – but also realistic – SARs will be developed. Once vetted, these fabricated SARs will be presented to and assessed by (different) SARs practitioners, including what (if any) follow-up action they would take. As such, the only cost to the practitioners from this is manpower and time. The first step in this process will be to generate a list of attributes/characteristics to describe SARs. These attributes might relate to the potential perpetrator (e.g., criminal background), the observed activity (e.g., terrorism pre-incident indicators), the reporter of the information (e.g., reliability), etc. This exercise will also assist the CREATE project team in better understand the real-world SARs operating environment in which the analysts work.

CREATE will then apply methods and tools from operations research, statistical modeling, decision theory, and risk analysis to analyze the responses of the SARs practitioners, including linking their responses to characteristics of the SARs (above) that they evaluated. Ultimately, the iSARs project will assist SARs analysts by:

1. gaining insights into how they structure the problem space and make decisions;
2. putting forth models, heuristics, and other methods to assist them in performing their duties; and
3. providing methods to automate many things that they are currently doing manually.

The SARs stakeholders will be continually and integrally involved throughout the project lifetime – through a series of meetings, interviews/surveys, and workshops. This will also maximize the project’s responsiveness to the needs of the stakeholder community, by better ensuring both that the deliverables are compatible with the current SARs operating environment, and also that they are something that the practitioners value and might actually use.

Although gaining access to past SARs has proven challenging, there is support from both local and national agencies, who have expressed a need for this research.

1.2. Project Status/Accomplishments

In Year 9, the project team worked closely with the OCIAC and JRIC to better understand the current analytic process employed for evaluating and acting on SARs. As a result of this engagement, two CREATE reports were produced (‘Plight of the Nationwide Suspicious Activity Reporting Initiative (NSI)’ and ‘SARs Flow-Chart, Information Sources, and the 8 Pre-Incident Indicators of Terrorist Attack’ – See Section 3.0 for additional details).

In addition, the project team engaged the DHS in an attempt to gain access to the National SARs Database as well as local and national law enforcement agencies to gain access to actual SARs. Although able to access classified SARs within the classified environment by cleared project
team members, the project team, unfortunately, was not able to access the DHS National SARs Database or gain access to unclassified, but sensitive SARs from local and national law enforcement agencies.

Given that access to actual SARs are critical to the success of this project, DHS and CREATE put a hold on the project until such access can be obtained.

2. Research Accomplishments
The project team has identified four main areas where SARs intelligence professionals have expressed interest, or:

1. greater tagging/categorization of SARs;
2. defining more clearly the threshold for what constitutes a meaningful SAR;
3. assessing the value of having acted upon SARs which were passed up the chain (i.e., to the FBI), but from which nothing ultimately came (the ‘intel black hole’);
4. devising a standardized way of measuring progress, successes, or failure of the overall SAR system – beyond the level of an individual SAR.

Gaining access to past SARs has been challenging, and so it was believed that the best was of acquiring data for the analysis is to have the intelligence professionals evaluate fabricated (but also realistic SARs) in a ‘real world’ test exercise environment. Unfortunately, we were not able to gain access to real SARs to help guide the development of the “virtual” SARs.

2.1. Research Products

<table>
<thead>
<tr>
<th>Research Product Metrics</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td># of non-peer reviewed publications and reports</td>
<td>2</td>
</tr>
<tr>
<td># of outreach presentations (non-technical groups, general public)</td>
<td>1</td>
</tr>
</tbody>
</table>

2.1.1. Non-Peer Reviewed Publications and Reports

CREATE NON-PEER REVIEWED PUBLICATIONS AND REPORTS

<table>
<thead>
<tr>
<th>Research Theme</th>
<th>Referred</th>
<th>Not Referred</th>
<th>PDF Sent to CREATE</th>
</tr>
</thead>
</table>

2.1.2. Outreach Presentations

CREATE OUTREACH PRESENTATIONS

<table>
<thead>
<tr>
<th>Research Theme</th>
<th>Referred</th>
<th>Not Referred</th>
<th>PDF Sent to CREATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nathaniel Heatwole, Michael Orosz, Erroll Southers. ‘Overview of CREATE Integrated Suspicious Activity Reporting (iSARs) Project.’ Single page research project synopsis and promotion. August 2013.</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3. Research Transition

3.1. Applied Relevance

Ultimately, the iSARs project will assist SARs analysts by:

1. gaining insights into how they structure the problem space and make decisions;
2. putting forth models, heuristics, and other methods to assist them in performing their duties; and
3. providing methods to automate what they are currently doing manually.

The project results could be of use to numerous entities in the intelligence and homeland security enterprises, including:

- JRIC and OCIAC intelligence fusion centers
- Local law enforcement and first responder agencies in southern California
  - Los Angeles County Sheriff’s Department
  - Los Angeles Police and Fire Departments
  - Los Angeles World Airport Police
  - Port of Los Angeles Police Department
  - Long Beach Police Department
  - Santa Ana Police Department (Orange County)
- Intelligence analysis and/or suspicious activity detection experts
  - Central Intelligence Agency (Center for the Study of Intelligence)
  - Coast Guard
  - Customs and Border Protection
  - Department of Homeland Security (Office of Information & Analysis)
  - Department of Justice (Office of Intelligence, Federal Bureau of Prisons)
  - Federal Bureau of Investigation
  - Naval Postgraduate School
  - Secret Service
  - Transportation Security Administration (Behavior Detection Officers)
  - Treasury Department (financial SARs and the Bank Secrecy Act of 1970)

3.2. Collaborative Projects

PortSec/InfraSec: The plan is to eventually make SARs available to the risk assessment engine(s) used in the PortSec/InfraSec technology.

4. Education

<table>
<thead>
<tr>
<th>Education Initiatives (Please detail below)</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td># of students supported (funded by CREATE)</td>
<td>1</td>
</tr>
<tr>
<td># of students involved (funded by CREATE + any other programs)</td>
<td>2</td>
</tr>
<tr>
<td># of students graduated</td>
<td>0</td>
</tr>
<tr>
<td># of student theses or dissertations</td>
<td>0</td>
</tr>
<tr>
<td># of contacts with DHS, other Federal agencies, or State/Local (committees)</td>
<td>2</td>
</tr>
<tr>
<td># of existing courses modified with new material</td>
<td>0</td>
</tr>
<tr>
<td># of new courses developed</td>
<td>0</td>
</tr>
<tr>
<td># of new certificate programs developed</td>
<td>0</td>
</tr>
<tr>
<td># of new degree programs developed</td>
<td>0</td>
</tr>
</tbody>
</table>
Project team members (Nathaniel Heatwole, Isaac Maya) met with Ashley Anderson (DHS Office of Intelligence and Analysis), Alex Carrillo and Alberto Martinez (OCIAC), and Robert Perez (Santa Ana Police Department) at the OCIAC fusion center in Orange, CA, in November 2012. A one-page synopsis of the iSARs project was also sent to all of the above persons in August 2013. The students on the project include:

<table>
<thead>
<tr>
<th>CREATE STUDENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Last Name</strong></td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>1. Perez</td>
</tr>
<tr>
<td>2. Kordbach</td>
</tr>
</tbody>
</table>

5. Outreach

<table>
<thead>
<tr>
<th>Outreach Initiatives</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td># of memberships in major DHS-related Committees</td>
<td>1</td>
</tr>
<tr>
<td># of contacts with DHS</td>
<td>1</td>
</tr>
<tr>
<td># of contacts with other Federal agencies, or State/Local (committees)</td>
<td>3</td>
</tr>
<tr>
<td># of contacts with State/Local (committees)</td>
<td>0</td>
</tr>
</tbody>
</table>

Project team members (Nathaniel Heatwole, Isaac Maya) met with a DHS official (Ashley Anderson, Office of Intelligence and Analysis), various SARs intelligence professionals (Alex Carrillo, OCIAC; Alberto Martinez, OCIAC), and a SARs analyst from a local law enforcement agency (Robert Perez, Santa Ana Police Department) at the OCIAC fusion center in Orange, CA, in November 2012 to discuss the nature and challenges of the SARs operating environment, and to formulate the specific goals of the CREATE iSARs project. A one-page synopsis of the iSARs project was also sent to all of the above persons in August 2013.

Project team members (Michael Orosz, Erroll Southers) met with JRIC officials to review classified SARs and discuss SARs challenges.

Membership in Major DHS Related Committees, Years 1-9

<table>
<thead>
<tr>
<th>MEMBERSHIP IN MAJOR DHS-RELATED COMMITTEES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committee</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>Michael Orosz – TSA Pre-Check Screening Committee</td>
</tr>
</tbody>
</table>

Meetings with External Organizations, Years 1-9

<table>
<thead>
<tr>
<th>MEETINGS WITH EXTERNAL ORGANIZATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Joint Regional Intelligence Center (JRIC)/Joint Terrorism Task Force (JTTF)</td>
</tr>
<tr>
<td>- Orange County Intelligence Assessment Center (OCIAC)</td>
</tr>
<tr>
<td>- US Coast Guard (USCG)</td>
</tr>
<tr>
<td>- InfraGard (Sacramento)</td>
</tr>
</tbody>
</table>