ACKNOWLEDGEMENTS

INSA CHAIRMAN
Ambassador John Negroponte

INSA ADVISORS
The Honorable Charles E. Allen, Senior Intelligence Advisor
Ambassador Robert Joseph, Senior National Security Advisor

INSA STAFF
Ambassador Joseph DeTrani, President
Chuck Alsup, Vice President for Policy
Jeff Lavine, Director of Administration & Management
Ryan Pretzer, Policy and Public Relations Manager
Elie Berman, Research Intern
Rebecca Hazlett, Research Fellow
Laura Wilkinson, Research Intern

HOMELAND SECURITY INTELLIGENCE COUNCIL (HSIC)
Caryn Wagner, INSA HSIC Chair

EDITORIAL REVIEW
Joseph M. Mazzafro, CSC

HSIC TABLETOP EXERCISE PLANNING COMMITTEE
Caryn Wagner, INSA HSIC Chair
Timothy Curry
Bob Hooks, TASC, Inc.
Dennis Hunt, URS Federal Services, Inc.
Steve Landry, URS Federal Services, Inc.
Karen Morr, Leidos
Jordan Renga
Ranee Rotter, CSC
David Sawczuk, URS Federal Services, Inc.
Charlie Shaw, Charles E. Shaw Technology Consulting, Inc.
Judy Smith, Exelis
Tony Spadaro, Spadaro & Associates
John Wherry, Exelis
Megan Woolsey

TABLETOP EXERCISE PARTICIPANTS

• Information Sharing and Analysis Centers
  ◦ Financial Services
  ◦ Real Estate
• National Counterterrorism Center
• Office of the Director of National Intelligence
  ◦ Program Manager of the Information Sharing Environment
  ◦ Office of Partner Engagement
• Royal Canadian Mounted Police, Federal Policing Criminal Operations
• State Law Enforcement
  ◦ Michigan Intelligence Operations Center
  ◦ North Carolina Fusion Center
• U.S. Department of Homeland Security
  ◦ Customs and Border Protection
  ◦ Federal Emergency Management Agency
  ◦ Office of Intelligence and Analysis
• U.S. Department of Justice
  ◦ Federal Bureau of Investigation
  ◦ National Security Division
• U.S. Department of State

Moderator: Ted Macklin, TOMAR Research, Inc.

TABLETOP EXERCISE SPONSORS
Deloitte
Spadaro & Associates
Exelis

INSA SUPPORTS A HEALTHY PLANET
INSA White Papers are printed on recycled paper that is 50% recycled content including 25% post consumer waste.
EXECUTIVE SUMMARY

The Intelligence and National Security Alliance’s Homeland Security Intelligence Council (HSIC) conducted a tabletop exercise at the Center for Strategic and International Studies in Washington, D.C., on April 10, 2014. Played out in a roundtable environment and using a fictional scenario, the exercise was designed to examine existing information sharing policies and procedures among a wide variety of stakeholders in the context of a homegrown violent extremist (HVE) threat. It was the intent of the exercise to identify processes and systems that work well, others that may require clarification, and any that require further study and dialogue. Scenario participants included representatives from the federal government, state government, Information Sharing and Analysis Centers (ISACs), and the Royal Canadian Mounted Police.

The fictional scenario involved a Canadian citizen arrested by U.S. Customs and Border Protection (CBP) officers after attempting an illegal entry to the U.S. with a specialized moisture gauge containing radioactive material. After questioning, the Canadian citizen revealed he was paid to bring in multiple gauges and one gauge was already in the possession of unknown buyers in the U.S. It was initially unclear whether the plotters were domestic, foreign or foreign-inspired, and what the target of any device might have been.

In response to the scenario, participants discussed topics such as how and when specific agencies become involved in the developing situation, the processes for information sharing among agencies and between levels of government, the high threshold level for issuing a National Terrorism Alert System (NTAS) alert, how agencies handle press leaks and communicating with the public, and how agencies share information with each other and with the public at the culmination of the situation.

Participants offered several key takeaways after the exercise:

- Strengthening relationships prior to an incident is paramount;
- Better ways should be found to engage the private sector;
- Officials must be prepared to share information publicly at any stage of a developing situation;
- Communications between federal, state, and local law enforcement, while robust, could still be improved;
- It may be time to reconcile Suspicious Activity Reporting (SAR) reportable behaviors with what has been learned about HVEs over the past decade.
The Tabletop Exercise highlighted several processes that seem to function well:

1. The FBI-led process that initiates a series of Threat Credibility Evaluations (TCEs) in response to a potential weapons of mass destruction (WMD) threat as codified in national policy seems well designed to evaluate WMD threats to initiate processes such as the FBI-led Nuclear Radiological Strategic Group (NRSG) that keeps all the key stakeholders informed and to ensure an appropriate response to an evolving threat.

2. The National Counterterrorism Center (NCTC) is engaged from the beginning but takes no action until there is a clear foreign nexus. This process is a good way to ensure civil rights and civil liberties are protected while ensuring the NCTC is ready to act if and when warranted.

3. The outreach mechanisms to state, local, tribal, and territorial (SLTT) law enforcement partners are quite robust and well exercised, particularly in comparison to the mechanisms for the private sector. While there was some question about the ability to maintain the necessary level of communication in a rapidly evolving situation, it was clear that there was a solid framework to work with.

It may be prudent to review the NTAS system to see if there is a better mechanism for formal communication with the American people, perhaps one that has lower thresholds for activation…

The HSIC offers six recommendations to help improve information sharing across the Homeland Security, Law Enforcement (LE), and Intelligence Community (IC) enterprises. These recommendations are based upon insights developed during the exercise planning process and participant discussions during the tabletop exercise.

1. Re-examine Suspicious Activity Reporting Guidelines to ensure that known HVE behaviors are incorporated.

2. Establish the practice of developing communications strategies in parallel with operations strategies on the assumption that leaks will happen.

3. Review communications mechanisms with the American public: is the NTAS system viable? Is another mechanism needed?

4. Review mechanisms employed to communicate with the states during rapidly evolving situations.

5. Review and possibly integrate federal mechanisms for conducting private sector outreach and for receiving information from the private sector.

6. Clarify countering violent extremism (CVE) roles and responsibilities and build appropriate linkages to LE and information sharing systems.

INSA’s first-ever Tabletop Exercise served as a useful tool for evaluating current practices and procedures in the event of an HVE threat. These findings and recommendations will be used to inform future research and activities of the INSA Homeland Security Intelligence Council.
MISSION, GOALS AND OBJECTIVES OF THE TABLETOP EXERCISE

The INSA Tabletop Exercise was designed to examine existing information sharing policies and procedures among a wide variety of stakeholders in the context of a homegrown violent extremist (HVE) threat. The purpose was to identify processes and systems that work well, others that may require clarification, and any that require further study and dialogue. The exercise was designed with specific objectives in mind to illuminate opportunities to enhance existing information sharing policies and procedures.

The first objective was to examine how federal, state, and local law enforcement officials and analysts share threat, suspicious activity, and information on U.S. persons; how they levy collection/information requirements; and how they produce intelligence reports on HVE threats.

There were several key issues to consider in the first objective. One key issue was to find out how well the various federal elements, in coordination with the state and local elements, understood their roles and responsibilities and consider if the current information sharing policies and procedures were optimized for an HVE threat. Another was to examine how well the behaviors codified in the National Suspicious Activity Reporting (SAR) Initiative correspond to what we know of the HVE threat, as well as determine where the regional boundaries associated with these organizations are, if they correspond, or if they create potential inhibitors.

The second objective was to examine how and what information is shared between Canada and the United States on U.S./Canadian persons and suspicious, transborder activity. Key issues considered in this objective were: could information be expeditiously shared between the Canadians and Americans in a border-crossing scenario, and how would procedures change if the border incident was not at a point of entry, but perhaps in a maritime environment.

The third objective was to examine how the Information Sharing and Analysis Centers (ISACs) – represented in the scenario by the Financial Services ISAC and the Real Estate ISAC – received and shared information, both with the federal government and with the relevant state and local fusion centers. Considered in this objective were whether or not the ISACs knew where and from whom they would receive information in a fast-breaking investigation that involved them – as opposed to more strategic information on long-term threat vectors – and if they were appropriately plugged in to both federal and SLTT networks.

NATIONWIDE SUSPICIOUS ACTIVITY REPORTING (SAR) INITIATIVE

The Nationwide SAR Initiative (NSI) is a collaborative effort by DHS, FBI, and SLTT law enforcement partners to prevent terrorism and other criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information.

Collaboration, stakeholder outreach, and technology are key components of the NSI campaign. Efforts between federal, state, and local law enforcement organizations nationwide ensure information is shared at all levels to keep the homeland safe from threats. The NSI takes all necessary steps to ensure Americans’ privacy and civil liberties are protected throughout the process.

INFORMATION SHARING & ANALYSIS CENTERS (ISACS)

ISACs are trusted entities established by critical infrastructure and key resources (CI/KR) owners and operators to provide comprehensive sector analysis, which is shared within the sector, with other sectors, and with government via Sector Coordinating Councils. Services provided by ISACs support risk mitigation, incident response, alert and information sharing. Member benefits vary across the ISACs and can include: access to a 24/7 security operations center, briefings, white papers, threat calls, webinars, and anonymous CI/KR Owner/Operator reporting. Two ISACs participated in the Tabletop Exercise: the Financial Services ISAC (FS-ISAC) and the Real Estate ISAC (RE-ISAC).
The fourth and final objective was to examine how existing mechanisms can be used to effectively communicate with the public in the event of a potential HVE threat. The key issue considered in this objective was under what circumstances would it be constructive, rather than counterproductive, to issue a National Terrorism Alert System (NTAS) alert.

**METHODOLOGY AND EXECUTION**

Development of the exercise scenario was based on the exercise objectives and issues associated with each objective. The Council’s research into the identified issues led to a scenario involving a radiological dispersal device (RDD) threat that is neutralized prior to detonation. The threat was to the financial sector from a group of HVEs, with cross-border involvement of a Canadian national. Council members reviewed the available literature on RDDs, HVEs, and intelligence sharing, interviewed a number of experts in these fields, and added their own insights to the development of the scenario.

HSIC’s research and discussions about the scenario and key question development culminated in the final scenario used for the exercise:

In mid-April 2014, U.S. Customs and Border Protection (CBP) officers discovered a specialized moisture gauge for construction use in the possession of a Canadian citizen who they detained due to illegal entry as the Canadian attempted to cross into the U.S. via the Detroit River. CBP officers ran the Canadian’s information through criminal and terrorist databases and did not find derogatory information. The Canadian initially refused to answer questions regarding why he had the device and why he was bringing it into the U.S. Instead he asked permission to consult the Canadian consulate and a lawyer.

CBP officers were concerned about the device because it contained radioactive material and they believed the Canadian may have been illicitly trafficking it into the U.S. for an unknown purpose, possibly even for a terrorist event. Officers called the local Joint Terrorism Task Force (JTTF).

**NATIONAL TERRORISM ADVISORY SYSTEM (NTAS)**

The NTAS replaced the color-coded Homeland Security Advisory System (HSAS). This system was intended to more effectively communicate information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector.

NTAS includes both imminent and elevated threat warnings. An imminent threat signals a credible, specific, and impending terrorist threat against the United States, whereas an elevated threat warns of a credible terrorist threat. DHS, in collaboration with other federal entities, decides which NTAS alert will be issued and when.

NTAS Alerts are distributed via the official DHS NTAS webpage, email alerts, data feeds, web widgets and graphics, as well as social media. Alerts also are shared in both public and private spaces, such as transit hubs and government buildings.
After several hours in detention, and at the suggestion of his lawyer, the Canadian revealed to JTTF agents that he had been paid to bring two moisture gauges to anonymous buyers in the Detroit area. Two days before his detention he had dropped off a separate moisture gauge in a park in the suburbs of Detroit. The Canadian had no knowledge of his buyers’ intended use of the devices, but he suspected the gauges might be used for an illegal purpose based on the availability of such devices in the U.S., the amount of money he was being paid, and the communications security the anonymous buyer implemented.

The disruption of the threat was accomplished by utilizing a mix of state, local, and federal information; investigation into the Canadian and his contacts; and community reported SARs.

To maximize the interaction between participants, the exercise was conducted in a roundtable format at the Center for Strategic and International Studies on April 10, 2014. The timeline of the fictional scenario was divided into three modules, and each module included several discussion questions for the exercise participants to consider. Mr. Ted Macklin, president of TOMAR Research, Inc., acted as the exercise facilitator, guiding participants through the modules and directing discussion questions to the appropriate participants. Mr. Macklin is an experienced exercise facilitator, recognized as a leader in homeland security preparedness, operational response, and exercise facilitiation.

Each exercise participant and observer was provided with an exercise binder, which included scenario descriptions, timelines, and discussion questions for each module, as well as an appendix in the back with additional information on the suspects and how they became radicalized, maps of locations relevant to the exercise, information on radiological dispersal devices, the Nationwide Suspicious Activity Reporting Initiative (NSI), the NTAS Public Guide, and a watchlisting presentation. Additional information and scenario injects were provided to the exercise participants via projected PowerPoint slides and inject handouts.

### WATCHLISTING

The watchlisting process is initiated when an IC member submits derogatory information on a known or suspected terrorist (KST) for inclusion in a U.S. Government terrorism-related database. All IC members may submit derogatory information on international KSTs to NCTC, which maintains a database that feeds the Terrorist Screening Database. Information on domestic KSTs is submitted by the FBI to the Terrorist Screening Center (TSC) for inclusion in the Terrorist Screening Database (TSDB). KSTs must meet the reasonable suspicion standard for inclusion in the TSDB. KSTs must have a measurable biometric or at least a last name and one other identifier before they can be included in the TSDB, which provides unclassified identifiers to multiple U.S. government screening systems.
Exercise participants included:

- Information Sharing and Analysis Centers
  - Financial Services
  - Real Estate
- National Counterterrorism Center
- Office of the Director of National Intelligence
  - Program Manager of the Information Sharing Environment
  - Office of Partner Engagement
- Royal Canadian Mounted Police, Federal Policing Criminal Operations
- State Law Enforcement
  - Michigan Intelligence Operations Center
  - North Carolina Fusion Center
- U.S. Department of Homeland Security
  - Customs and Border Protection
  - Federal Emergency Management Agency
  - Office of Intelligence and Analysis
- U.S. Department of Justice
  - Federal Bureau of Investigation
  - National Security Division
- U.S. Department of State

Throughout the course of the exercise, each of the participants responded to the scenarios presented by adding thoughtful insights based on their particular experiences and their organization’s protocols. The fusion of federal, state, local, and Canadian participation allowed for an in-depth discussion regarding when, how, and why organizations respond to HVE threats as they do. The next section presents an overview of the scenario the exercise participants faced, and discusses how the various stakeholders responded.

SUMMARY OF EXERCISE DISCUSSION

Full details of the scenario used in the exercise can be found in the appendices of this report. The following is a summary of the exercise participants’ discussion throughout the three exercise modules.

MODULE 1 DISCUSSION SUMMARY

During Module 1, CBP officers detain a Canadian attempting to cross the Detroit River with a soil density gauge containing radioactive material, and the authorities learn the suspect had already dropped off a gauge to unknown buyers in the Detroit, Michigan area. Discussion during Module 1 centered on two main topics: how and when specific agencies became involved in the developing situation, and the processes for information sharing among agencies and between levels of government. CBP is first on the scene and immediately sends any radiological information obtained from the gauge to the 24/7 laboratory for analysis and also begins an investigation into available data on the suspect’s previous border crossings, immigration and law enforcement history, and contact information. CBP alerts the FBI, which dispatches a field division WMD coordinator (WMDC)
to begin an FBI WMD-counterterrorism investigation and coordinate outreach with federal and state partners as well as the private sector. CBP also receives support from DHS through its National Operations Center (NOC) which addresses such interdictions on a 24/7 basis.

The FBI WMDC alerts the field division JTTF who will assume the FBI WMD-CT investigation, and alerts the WMD Directorate who will conduct an immediate Threat Credibility Evaluation (TCE) with all relevant stakeholders, including the Department of Energy, to evaluate the credibility of the plot and feasibility of the device in question. Because this likely relates to a WMD crime or act of terrorism, the FBI will assume the lead over the investigation and elicit support as necessary from the NCTC and Michigan Intelligence Operations Center. Through the JTTFs, state and local partners are provided with situational awareness and begin to investigate the incidents. Other state and local law enforcement are informed initially on a need-to-know basis to help contain intelligence leaks. At the national level, the FBI informs interagency partners such as DHS, FEMA, and the State Department through an operational coordination mechanism or crisis action team called the Nuclear Radiological Strategic Group (RNSG). The interagency RNSG stands up at FBI Headquarters within the Strategic Information Operations Center. This group of Subject Matter Experts (SMEs) conducts many activities which includes the production of a threat profile that is tailored to many audiences to include border protection, critical infrastructure, law enforcement, international partners, etc. The RCMP will be engaged early on via CBP to conduct indices checks on the detained Canadian citizen, and will be prepared to escalate their involvement as the investigation requires. The FBI legal attaché within Canada will also engage RCMP and coordinate the United States criminal investigation.

The FBI and DHS maintain close communication on a daily basis, ensuring that collaboration during the initial phases of an HVE investigation or incident is smooth and communication is regular. Because similar incidents have occurred over the past decade, there are protocols now in place to follow. DHS intelligence officers at the state level ensure that there is a pipeline of information from the federal to local level, and border task forces share information with their Canadian counterparts. Not all pertinent intelligence is shared due to operational security and to protect the investigation; however, information sharing does happen in real time to maintain situational awareness among agencies involved.

**MODULE 2 DISCUSSION SUMMARY**

During Module 2, the White House and several federal agencies discuss the situation and determine the moisture gauge could be used in a low-level and panic-inducing attack against a homeland target; a press leak about the Canadian’s detention also occurs. Discussion during Module 2 began with considerable agreement among participants that an NTAS alert should not be issued. Instead, the FBI begins a full-field dual Counterterrorism and WMD investigation focused on gathering intelligence, CBP puts its agents on high alert by increasing border checks and patrols, and DHS, with the FBI, issues a Joint Intelligence Bulletin (JIB) that includes information on the gauge device and how it might be used to make an RDD for distribution to state and local partners at the SECRET level.

Following the news leak – which misrepresents the threat as nuclear rather than radiological – the consensus among exercise participants was that an NTAS alert still should not be issued. In order to reduce fear and panic among the American public, the FBI Public Affairs Department publicly verifies there is no evidence of loose nuclear material. The Michigan fusion center engages the private sector through coordination with directors of security. Key participants would work with the White House Public Affairs Department to coordinate on language for media releases, most importantly a clarification to eradicate the word “nuclear” and consideration to ensure preservation of the investigative process.

Despite the fact participants did not believe it was warranted, the scenario included an NTAS issuance in the wake of the press leak. After the alert is issued, the Michigan fusion center would work with its various federal and local partners to coordinate the flow of information to the lead investigative agency. In this particular case, the FBI requested the state fusion center to triage all incoming information based on consideration for follow-up action. The FBI promotes its 1-800 tip line for the public to report suspicious activity and the DHS publicizes the “See Something, Say Something” campaign. Financial and Real Estate ISACs promote situational awareness and release alerts to members.
The press leak and subsequent NTAS alert results in a high volume of calls and tips nationwide, and agencies fear their current resources will not be sufficient to meet the influx of information.

**MODULE 3 DISCUSSION SUMMARY**

During Module 3, tips from the general public lead the authorities to suspect three radicalized siblings of planning an attack on the homeland, an RDD is discovered and successfully disabled by authorities, and the three suspects are apprehended. Discussion during Module 3 focused on two essential elements for counteracting the threat: investigations and operations. As mentioned before, the FBI and DHS remain cognizant of sharing information in a measured way to reduce the likelihood of leaks and to maintain the integrity of the investigation.

The investigation proceeds quickly with the new information resulting from the NTAS alert. The FBI enhances its coordination with the RCMP and State Department and issues an all-points bulletin to find the location of the suspects. The FBI also integrates InfraGard into its investigation to help with information sharing between the agencies and the private sector. The North Carolina Fusion Center stays in constant communication with FBI and DHS. With intelligence pointing to North Carolina or Michigan, DHS is likely to de-emphasize the threat for other regions of the country. With indications of foreign influence, the NCTC begins to review its holdings and takes a more active role in supporting the investigation.

Operational capabilities are also enhanced to ensure assets are in the field. The FBI sets up forward staging areas in Detroit and Charlotte, and states its enhanced SWAT team, Hostage Rescue Team, and its bomb technicians in both areas. The Attorney General, the Director of the FBI, and the FBI Field Division Special Agent in Charge direct the FBI operations to include the tactical and technical operations.

**KEY TAKEAWAYS OF PARTICIPANTS**

The need to develop strong communications plans and protocols was a point of emphasis for many participants, with respect to both engaging the pertinent government and private sector partners to ensure a robust investigation and the sharing of timely and accurate information with the media and public.

**Strengthening relationships is paramount.** Several participants stressed that relationships should be proactively developed amongst local, state and federal entities to foster trust and put collaborative mechanisms in place before threats and incidents arise. “Keep in mind that all these things start at a local level,” said one state-level participant. “Quicker resolution comes when information is smoothly communicated up the chain.” Moreover, the inherent public safety concerns that accompany a security threat – the threat of widespread public exposure to biological or chemical agents, for instance – would significantly broaden government engagement at nearly every level, making interagency coordination even more essential. Another participant said, “focus on the intersection of homeland security and public health.”
Engage the private sector. While government agencies and law enforcement would appropriately take the lead in investigations, the private sector is an integral partner, and, in many cases — as in this scenario — may be the target. Early and ongoing information sharing with the private sector must not be overlooked, several participants stressed.

“Leverage the private sector because we’re often the ones that see it on the ground first,” said one ISAC participant, who added that there are security-cleared individuals in the private sector who can offer additional assistance. “Industry will be a willing participant,” added a second ISAC participant.

One government official observed that information sharing should be a two-way street, with the private sector remaining in the loop on developments. “Continue to share the information and don’t just take their information and not inform them of progress,” he said.

Another government official noted the exercise was a good way to inform discussions on improving current information-sharing channels. “It’s not always pretty, it can be inconsistent, but it’s important to think about how the FBI can streamline information sharing with the private sector,” he said.

Be prepared to share information publicly — ready or not. While the issuance of an NTAS alert may aid the investigation through the public’s involvement, it also opens the door to the media spotlight. Organizations should work together to identify the threshold for sharing threat information publicly, as well as to develop a clear communications strategy to combat misinformation and speculation. “We move from ‘a need to know’ to ‘a responsibility to share’ once the NTAS [alert] comes to light,” said one federal-level participant. “Keep your communicators informed so we can provide the breathing space for agencies involved.” Added another participant, “Assume there’s going to be a leak, so be prepared.”

Communications between federal, state, and local law enforcement still needs work. Fusion centers — established as primary focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information among federal and SLTT partners — did not play a major role in the exercise due to how the play unfolded. As stated in national policy, terrorist threat-related information collected domestically, to include suspicious activity reporting involving suspected federal crimes of terrorism, will be shared comprehensively and immediately to the FBI JTTFs so that threats can be investigated and resolved. It was noted that this would have been different had the scenario focused on an incident rather than on the investigation of a potential terrorist act. However, some participants came away with questions regarding when fusion centers would enter the investigative process, and how and when they would receive information from the national level. “What would the information sharing be like from the FBI to the fusion centers prior to an NTAS [alert]?” asked one participant. “[We have] no experience with this since it has never happened before.”

Reconcile SAR reportable behaviors with what we have learned about HVE. Participants agreed it was important to take another look at the SAR reporting guidelines, or as one of them put it, “cross walk what we know about HVE indicators and the SAR behaviors that are captured in that.” Another noted that “our biggest challenge is homegrown violent extremists; they are very difficult to interdict,” reinforcing the importance of maximizing the likelihood that indicators will be recognized and reported.
AREAS THAT WORKED WELL

1. The FBI-led process that initiates a series of TCEs in response to a potential WMD threat seems well designed to keep all the key stakeholders informed and to ensure an appropriate response to an evolving WMD threat. It is implemented numerous times each year, and thus has become an institutionalized response. It allows all stakeholders to weigh in on the credibility of the threat and discuss appropriate investigative and operational responses, and is a way to keep elements such as the NCTC and FEMA in the loop even though they may not be required to take actions until later in the process.

2. As a matter of policy, the NCTC begins tracking incidents that reasonably could have a foreign terrorism nexus upon notification, but generally takes no analytic or coordination action unless/until a foreign nexus is identified. This is a good practice, ensuring civil rights and civil liberties are protected while ensuring the NCTC is ready to act if and when warranted. Under law, the NCTC is the primary all-source analytic element for the terrorist threat, but as a Title 50 organization, generally deals with threats with a foreign nexus, versus purely domestic terrorist acts. In this scenario, however, as in other real world scenarios, it is often difficult to tell at the beginning what the actors’ motivations might be or whether they were influenced by foreign ideology or even directed from overseas. Bringing the NCTC into the game cold after a foreign nexus is discovered is not very efficient, especially if there is an active plot that could involve perpetrators at large in the United States. The mechanisms discussed in the Tabletop Exercise seem prudent and appropriate to keep the NCTC in the loop on threats as they arise so they can engage more fully when a foreign nexus is discovered.

3. The outreach mechanisms to SLTT law enforcement partners are quite robust and well exercised, particularly in comparison to the mechanisms for the private sector. While there was some question about the ability to maintain the necessary level of communication in a rapidly evolving situation, it was clear there was a solid framework to work with. Many other reports and studies have focused on the Information Sharing Environment, the role of the fusion centers, and the responsibilities of the various federal elements to share information in a structured way with SLTT partners. Thus, we will not belabor the issue, other than to say that our recommendations are meant to improve an already functioning system.

RECOMMENDATIONS FOR FURTHER EXAMINATION

The following six recommendations are to help improve information sharing across the Homeland Security, Law Enforcement (LE), and Intelligence Community (IC) enterprises. These recommendations are based upon insights developed during the exercise planning process and participant discussions during the tabletop exercise.

Re-examine SAR Guidelines to ensure known HVE behaviors are incorporated:
The current guidelines for suspicious activity reporting were developed using an interagency process that included many stakeholders, including the privacy and civil liberties communities although they did not formally sign off on the resulting guidelines. The
guidelines include 16 reportable behaviors designed to ensure that reports are not based on profiling or reporting on constitutionally protected activities. However, as time has gone by, the IC and LE communities have produced analysis documenting the behaviors of those who have crossed the line from constitutionally protected speech to violence and engaged in terrorist activities. While it is notoriously difficult to predict who will cross that line and become homegrown violent extremists, current analysis has produced some indicators that are commonly, if not universally, seen as these individuals go down the path to violent extremism. It may be time to review the current NSI behaviors to ensure that these known HVE indicators are adequately reflected in the guidelines, while still preserving privacy and civil liberties.

Establish a process for developing communications strategies in parallel with operations strategies on the assumption that leaks will happen:
The INSA Tabletop Exercise was unusual, if not unique, in that it incorporated a press leak into the exercise itself and examined how the leak would impact an ongoing investigation and associated law enforcement activities, as well as how and with whom information would be shared as a result. Participants agreed leaks have become part of the operational landscape, and responses to potential or actual terrorist incidents must include a sophisticated communications strategy from the very beginning. The strategy must include what will happen if or when a leak occurs. Proactive notifications of key state and local personnel and members of Congress should be considered in order to avoid scrambling to communicate with these individuals in the immediate aftermath of the leak. Ironically, these individuals are frequently not informed in order to prevent leaks while the investigation is ongoing. Whether they are notified in advance or not, a robust plan that includes talking points, established communications channels, and prepped briefing teams should be part of the communications strategy. We should constantly be asking, “What is the plan if we look up and this is on the network news?”

The corollary is that sharing information about a serious threat, even among only federal law enforcement and select others, will result in a leak. But the government cannot be effective without sharing that information. If the federal government could publicly address the threat before the media crafts its own narrative, it could stay in front of the issue rather than react and defend. The American public is more resilient than it is given credit for. In an era of instant communication and citizen activism it might be better, at least in some scenarios, to harness that energy than hope they won’t find out – although resources for dealing with a high-volume engagement with the public would have to be trained and scaled accordingly. This is a model that has been used successfully and could be considered for serious threats.

Review communications mechanisms with the American public:
The discussion surrounding the issuance of the NTAS message was very interesting. The NTAS was designed to replace the much-maligned, color-coded Homeland Security Advisory System that was put in place after the attacks of 9/11. The NTAS attempted to deal with some of the shortcomings of the previous system, establishing thresholds for “elevated” or “imminent” threat situations, and ensuring that alerts would be issued for finite – and generally short – periods of time. It was predicated upon unclassified communication with the American public. In practice, the NTAS has proved unexpectedly difficult to employ for a variety of reasons. Intelligence generally does not supply the details necessary to establish when an attack might happen and there are frequently complications from notifying the American public about a threat that is not well understood or defined. The result is that no unclassified NTAS alert has ever been issued and there may never be one. It may be prudent to review the NTAS to see if there is a better mechanism for formal communication with the American people, perhaps one that has lower thresholds for activation and that accommodates more of DHS’s homeland security missions, rather than being restricted to counterterrorism. A few participants mentioned that a mechanism like this could be very helpful in a public health or natural disaster scenario. In the meantime, the limited utility of NTAS for the current terrorist threat environment puts a premium on the strategic communication strategy mentioned earlier.

Review mechanisms employed to communicate with the states during rapidly evolving situations:
While it was apparent that much progress has been made in developing procedures for joint communication with SLTT law enforcement, some participants expressed doubt that in a fast-moving situation their agencies would have the bandwidth to keep the SLTT partners appropriately
informed. It was also not clear that there was one identified mechanism or conduit for information sharing. While the FBI/JTTF would have the lead for ongoing terrorism investigations and for sharing information with local elements as needed for the case, if there were other types of information or coordination required, that process seems less clear. In the wake of the Boston Marathon bombing, DHS is exploring formalizing the role of its deployed intelligence officers (IOs) in performing this function. For this to be effective it would have to be recognized first by DHS components and then by interagency partners. While the exercise did not include information sharing in a post-detonation scenario, it is worth exploring the need to plan for performing this critical function. Another issue worth exploring is whether any mechanism established for this purpose could serve another purpose that was discussed during the exercise: hand-off between different geographic regions and potentially surge support from one region to another in a flexible, near-real-time manner.

Review and possibly integrate federal mechanisms for conducting private sector outreach and for receiving information from the private sector:

Representatives from two ISACs participated in the exercise and provided a valuable perspective on information sharing with critical infrastructure. The ISACs were created by Presidential Decision Directive 63 in 1998, and further codified in the NIPP, the National Infrastructure Protection Plan. Each of the 16 ISACs has a staff that is responsible for representing the sector’s equities and requirements with the appropriate government referent in the Sector Coordinating Councils. The threat in this exercise was to the financial sector – specifically banks – and it was not clear how this might have been communicated to the entire sector or a geographic sector as opposed to an individual bank (which would have been done by the FBI incident to the investigation). The ISACs do not appear to be linked into the communications strategy for immediate, tactical threats, although they do routinely receive information about the strategic threat environment and evolving terrorist tactics, techniques and procedures from DHS. It was also not clear how information from the sector would find its way into the NSI space, and whether security officers are informed of the NSI behaviors and of other information that would better enable them to be force multipliers.

Clarify CVE roles and responsibilities and build appropriate linkages to LE and information sharing systems:

In our scenario, an imam in Detroit called a DHS IO to report his suspicions about a member of his congregation because he had met the IO at an outreach event and trusted him. A great deal of outreach to counter violent extremism has taken place in the Detroit metropolitan area, home to the largest Arab-American population in the U.S., and Minneapolis, which has a considerable Somali diaspora. This could be viewed as a success story, but it is not clear that there is a coherent approach to these outreach efforts, to include defining who is responsible for managing and overseeing it. The CVE program is defined as being a whole of government approach, which is very appropriate, except that someone has to have final responsibility for executive branch efforts to succeed. The importance of CVE and community outreach efforts in the current and future threat environment is such that revisiting this diffusion of responsibility might be warranted to ensure the desired outcome is achieved while respecting civil rights and civil liberties.
CONCLUSION

Exercises, such as the Tabletop Exercise discussed here, give stakeholders an opportunity to role play using established processes and determine if improvements can be made or if there are gaps that should be addressed. The HSIC recognizes that for the purpose of this exercise, participants may have been relying on established doctrine, policies, and procedures that are intended to provide clear command and control as well as communication between a variety of stakeholders. However, developments may occur too quickly to follow such policies in a real-world scenario.

During any crisis, informal methods of communication and workflow may develop, and are likely to be based on strong personal relationships within and between individuals and offices at different layers of government, the private sector, and the general public. Unfortunately, at the individual level these personal relationships have a few shortcomings. They may encourage stovepiping of information needed by other agencies or they do not contribute to institutional memory, leading to less-than-optimal operations. At the work unit level, those disadvantages become less apparent. Therefore, the HSIC encourages all homeland security stakeholders to encourage, maintain, and develop relationships between work units at a variety of government, private sector, and public levels to foster greater communication and increase the level of effort that may be applied to resolve any given crisis. At the same time, the Tabletop Exercise has identified areas for further exploration and improvement that support the development of processes and institutional memory that transcend individual relationships. The combination of sound processes and good relationships allow those processes to be effectively tweaked for every potential scenario, bolstering the interagency fight against terrorism.

APPENDICES (AVAILABLE ELECTRONICALLY)

Appendix A: Exercise Scenario Slide Deck
Appendix B: Exercise Scenario Timeline

ABOUT THE INSA HOMELAND SECURITY INTELLIGENCE COUNCIL:
The INSA Homeland Security Intelligence Council (HSIC) is focused on the topic of intelligence activities and information sharing required to protect the U.S. from significant threats. The Council is comprised of senior executives, past and present, from across government, law enforcement and industry who contribute to the homeland security enterprise.

ABOUT THE TABLETOP EXERCISE:
On April 10, 2014, INSA’s Homeland Security Intelligence Council, led by Council Chair Caryn Wagner, conducted a Tabletop Exercise at the Center for Strategic and International Studies in Washington, D.C. The exercise was designed to examine existing information sharing policies and procedures among a wide variety of stakeholders with the purpose of identifying areas that work well, others that may require clarification, and any that require further study and dialogue. The HSIC Tabletop Exercise Report Task Force used information from the exercise and participant discussion and feedback to develop the report published here.