

## Why Partnership Matters



**Zalmai Azmi**  
INMA Board of Directors  
*Nation's Capital IMA*

This month's terrorist attack in Mumbai is yet another reminder that the threat of terror is real and the terrorists can strike anytime at any target without any warnings. The terrorists have adopted new ways. They are indiscriminate in selection of their targets and they are more agile and flexible in the execution of their mission. They proved this by holding the city of Mumbai hostage for more than three days.

The United States is constantly threatened by those who challenge our national security and our way of life. Our national infrastructure remains vulnerable and the disruption of any element of the infrastructure will have a tremendous impact on our nation. In the last seven years within the United States the national security programs have undergone tremendous transformation. The military, federal, local, state, private sector and other agencies have sought new expertise in security with a commitment to the safety of our nation. However, the challenge goes beyond the expertise of any one agency. National security is not the job of a single agency or entity, it is a national mission and every individual has a role to play. That is why partnership matters.

Every agency and entity has expertise and resources that can be shared or leveraged by another. It could be anything: information, technical solutions, best practices, anything that can thwart another 9/11-like event. InfraGard in partnership with the FBI plays a critical role in providing the means for these agencies to collaborate and share information and best practices.

Information sharing is at the heart of our national security strategy. The Markel Foundation's first report highlighted the urgency for information sharing and presented a high level strategy. Since, the agencies have made tremendous progress in this area to include the creation of the Program Manager for Information Sharing Environment (PM-ISE) and information sharing Executives within some of the agencies. However, there is no specific maturity model or process by which the information sharing progress can be measured. The development of such a maturity model will help agencies to self evaluate and grade themselves. Based on that information they can set new goals and milestones for their information sharing programs.

Despite the progress in the information sharing environment, two major challenges still remain to be addressed. First, the National Information Exchange Model (NIEM) standards developed and championed by the law enforcement and homeland security communities need to be reconciled with DoD's Universal Core (UC). Second, a national set of standard information sharing policies must be implemented and enforced. These policies must be in compliance with the applicable laws that ensure the protection of US person data and the preservation of civil liberties.



There is a general consensus that technology has not been an impediment because many agencies have developed suites of tools for sharing information securely and expeditiously. For example, the FBI has made large investments in developing technical solutions that will benefit its partners in the law enforcement and intelligence communities and the private sector. Guardian is one such program, which is the main automated system for tracking terrorist threats and suspicious incidents and has been in production since 2004. An unclassified version of the Guardian application will go into production by the end of this year which will provide the community with a single web based tool to report suspicious activities. Per the FBI's policy every one of these incident reports will be reviewed, prioritized and appropriate action will be taken. The information will be shared with FBI partners as appropriate.

Like the FBI, other agencies also have made substantial investments in security related projects, technologies, and programs. The key to our success and protection of our nation from terror attacks is the timely sharing and leveraging of these capabilities. Trusted partnership plays a key role in making this happen.