

III. Share Information and Intelligence (I2)



If you see something, say something.

**Share Information
Gather Information
Distribute Information**

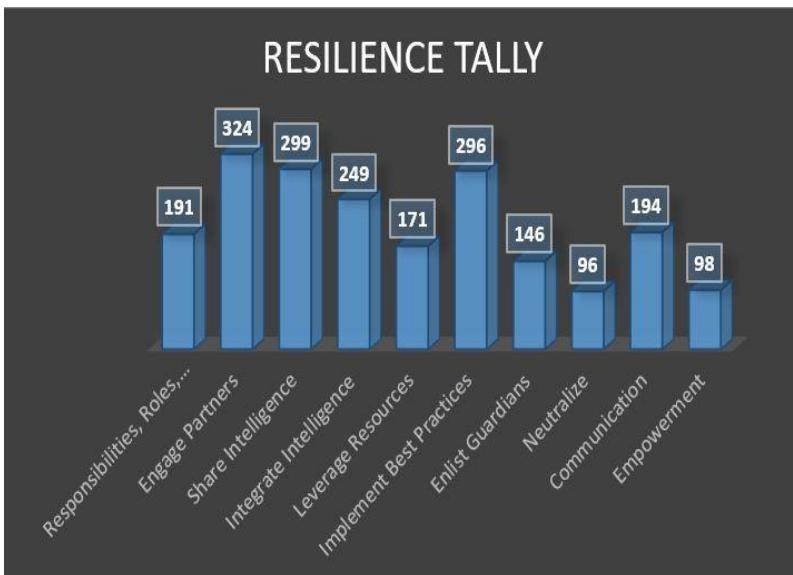
“TO GLOBALIZE A PROBLEM, WE NEED TO SPREAD AWARENESS OF THAT PROBLEM.”

- STEPHEN J. KRAMER, PRESIDENT OF THE STATE AGENCY

About

The third pillar of the R.E.S.I.L.I.E.N.C.E model is “Share Information and Intelligence” (I2). The main goal of this pillar is to encourage others to spread situational awareness about a potential threat towards a vulnerable community or a house of worship. It is important to share any information regarding that threat or any intelligence about handling the threat. Doing so will help in forming connections and contacts within vulnerable communities and houses of worship, as well as building their trust.

According to analysis of the 31 conducted interviews, “Share Information and Intelligence” has the 2nd highest count of 299 mentions, as shown in the graph below. This marks it the 2nd most important pillar of the model next to “Engage Partners”.



“We need to share and disseminate information about the threat. We need to emphasize on the importance of cooperation between law enforcement, the public, community, especially potential targeted communities and faith based leaders and organizations.”

- Ali Soufan, Former FBI agent

The Importance of Sharing Information & Intelligence

To collect and share information of potential threats, we must actively promote the reports of all hate communications. These may be directed at not only a single individual, but at a group of a specific demographic. For example, a faith-based community might be facing hate speech or physical threats. While these may not be hate crimes, they can lead to a hate crime. That is why it is important for us to increase awareness about them to prevent further damage from happening, especially towards houses of worship. This will give citizens a chance to prepare themselves against the threats or any potential escalation, building their resilience within their community.

Everyone may have different backgrounds and religious beliefs from each other, but we need to put these differences aside to expand our connections. This can range locally or nationally, but the more connections we form, the more information and awareness can be spread about potential violence. One can learn more about another faith by participating in interfaith councils and discuss about security trends and measures to protect houses of worship. One can also share their experiences in dealing with targeted violence to teach others how to handle a specific situation; if a suspicious person enters a house of worship, how can one spot them and drive them out? Whatever we do to communicate and share information with each other, we can form stronger bonds and resilience to protect ourselves.

“There's real value in networking with other faiths and obviously they have different religious beliefs, but in terms of security issues, and how to protect your houses of worship, there are a lot of commonalities that I think they can really profit from talking to each other those challenges.”

- John Farmer, Attorney General



It is important for the police and law enforcement agencies, both nationwide and worldwide, to be responsive to any kind of warning. They need to reach out to houses of worship and inform them any significant information about potential violence. By doing so, they can ensure the houses of worship that they are reliable authorities who can protect them. This can improve on not only how both the police and houses of worship can respond to various situations, but also how information can be properly distributed. For instance, one might feel uncomfortable about reaching out to the police and will instead reach out to someone at their local house of worship. If the information they tell indicates a potential threat, the house of worship can send out warning messages to their congregants from the police, as well as other houses of worship.

*“I think that we have a **multidimensional picture that’s operating through various vectors** and it’s becoming increasingly complex to counter those threats. It requires a **real sense of awareness amongst our public safety professionals and first responders as well as within the community itself.**”*

- Michael Masters, National Director of the Secure Community Network

However, sharing information about potential threats needs to be done accurately and reassuringly to avoid fear-mongering or spreading false information. Additionally, if one has enough precise information, one can use it to counterpoint any hateful communications or false information. Social media has a large impact in spreading such information, so it is also important to educate online users, especially children, on what kind of content is appropriate; if not, it must be reported to authorities, who must respond accordingly.

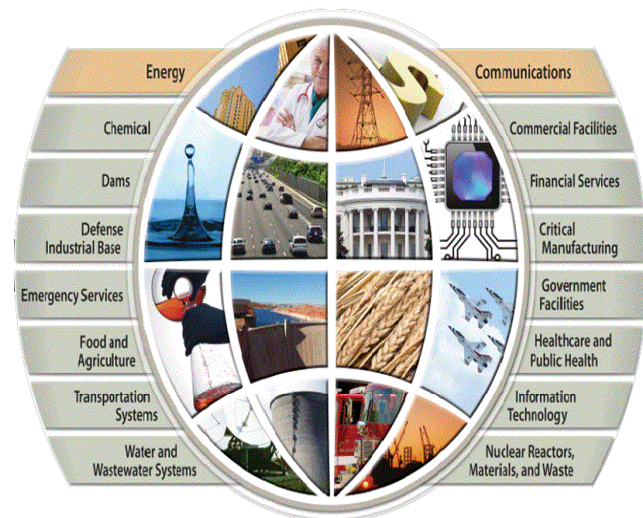
Outside of the police and law enforcement, there are many other organizations that frequently share various information for vulnerable communities. For instance, the Faith-Based Information Sharing & analysis Organization (FB-ISAO) is a security consortium for faith-based organizations and associations, along with houses of worship. It has frequently informed these organizations with relevant information and analysis about physical threats, cybersecurity issues, health outbreaks, natural disasters, etc. The FB-ISAO seeks to provide its members with their informational assets “to help reduce risk while enhancing preparedness, security, and resilience”. It has been a trusted partner among a faith-based network, showing that many organizations like this are willing to assist vulnerable communities by providing them the information they need to know. Thus, it is best to join such an organization to actively collect information of potential threats and share it to those who need it.

Examples of Information-Sharing Hubs

National

The following hubs directly interact with critical infrastructure owners and operators and the private sector:

- **Federal Bureau of Investigation Headquarters Elements (FBI HQ)**
- **National Cybersecurity and Communications Integration Center (NCCIC)**
- **National Infrastructure Coordinating Center (NICC)**
- **Information Sharing and Analysis Centers (ISACs)**
- **Information Sharing and Analysis Organizations (ISAOs)**
- **Sector Specific Ops Centers**




[Pictured above] A diagram of the many resources that ISACs gathers information about

The following hubs do not directly interact with owners and operators and the private sector, but have a role within the critical infrastructure security and resilience mission space:

- **DOT Crisis Management Center (CMC)**
- **Joint Counterterrorism Assessment Team (JCAT)**
- **National Counterterrorism Center (NCTC)**
- **DOD National Military Command Center (NMCC)**
- **FBI Strategic Information Operations Center (SIOC)**
- **FBI Terrorist Screening Center (TSC)**

Local and Regional

- **State or City Emergency Operations Centers (EOCs)**
- **FBI Field Offices**
- **State and major urban area Fusion Centers**
- **Information Sharing and Analysis Organizations (ISAOS)**
- **Law Enforcement Agencies**
- **Regional Cybersecurity Information-Sharing Networks**



*“WE HAVE TO ALWAYS STAY ONE STEP AHEAD OF
THE THREAT PICTURE. WE CAN’T JUST RESPOND
TO THE LAST ATTACK, WE HAVE TO ANTICIPATE
THE NEXT ONE.”*

- JEH JOHNSON, HOMELAND SECRETARY

Works Cited

"About Us." *FB-ISAO*. <https://faithbased-isao.org/about/>. Accessed 21 June 2019.