Improving the Value of Information Sharing
Geographically-Based Community ISAOs

Dr. Greg White
Executive Director
ISAO Standards Organization
EO 13691 described several possible types of ISAOs

“ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities. ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.”
Geographically-Based Community ISAOs

At last year’s IISC the ISAO SO stated that it felt that the “sweet spot” for ISAOs in the coming years.

- Help to build trust between organizations
- Raise awareness on Cybersecurity issues especially for SMBs
- Encourage more public/private partnerships
- Encourage information sharing between sectors within the SLTT
• Subject to growing number of cyber attacks
  • More high-profile attacks on states
  • Loss of millions of citizens PII
    • Social security numbers
    • DOB
    • Drivers license numbers
    • Payment card records
    • Tax data
  • These incidents have cost millions of dollars in clean-up costs, loss of revenue and public trust
Figure 4. States and territories reported the highest capability ratings in Public Information and Warning and the lowest capability ratings in Cybersecurity and Economic Recovery.
• No clear strategy to implement a cybersecurity program for local jurisdictions
  • Cybersecurity threat is not understood
    • What is the scope of the cyber threat?
    • How can it impact a community?
    • Traditional incident response personnel in a community including Emergency Management generally do not understand the threat cyber attacks pose.
  • Roles are not understood
    • Who in the community should be involved?
    • How can the public and private sectors work together?
    • What can the federal government provide for you?
Why Information Sharing is Important Across an SLTT

• UTSA has conducted research into community incident detection and response since 2012
• Developed a “Honey Community” to gather data on attacks on a small community
• Patterned our website after a number of other small community websites in Texas
• Connected to the Internet and sat back and watched…
Our Original Honey Community
Looking across multiple sectors is critical

- 3,060 IDS alerts generated by SNORT
- 55% of attacks can be seen as an attack on 1 or more sectors
- 45% of attacks were not attributed to a sector but the effort could be seen across the entire enterprise (the * entry above)
- Attacks against 1 sector appeared to re-appear later against another sector

Information Sharing Trifecta

NCRI
- Professional Organization
- Community Voice
- Public-Private Partnerships
- Vetted Memberships
- Information Sharing Mentorship
- Code of Ethics
- Compliance
- Forum
- Training
- Think Tank
- Secure Portal
- Committees
- Annual Conference

ISAO SO
- Repository
- Publications
- Standards
- Guidelines
- Surveys
- Website
- Volunteer Working-Groups

Geographically Based Community Based ISAO
- Information Sharing
- Public-Private Partnerships
- Marketplace
- Forums
- Training/Exercises
- Internships
- Secure Portal
- Messaging
- AIS/Operations Center
- NCCIC Seat
Questions?

Gregory B. White, Ph.D.
Greg.white@utsa.edu