IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

INTERNET SECURITY – INFORMATION SHARING AND ANALYSIS ORGANIZATION PILOT

ENABLING CYBER RESPONSE: FOCUSING ON BI-LATERAL AND REGIONAL CYBERSECURITY INFORMATION SHARING

State, local, tribal, and territorial (SLTT) governments and organizations depend on information technology systems and computer networks for essential operations. These systems face large and diverse cyber threats that range from unsophisticated criminals to technically competent intruders using state-of-the-art intrusion techniques. Many malicious attacks are designed to steal information and disrupt, deny access to, degrade, or destroy critical information systems. The Cybersecurity and Infrastructure Security Agency (CISA) works with SLTT governments to promote the adoption of common policies and best practices that are risk-based and able to effectively respond to the pace of ever-changing threats.

Under Grant Award Number DHS-18PDSA000002-01-00 (SLTT Internet Security - Information Sharing and Analysis Organization Pilot), CISA awarded a cooperative agreement to the Los Angeles Cyber Laboratory (LACL) to help regional SLTT governments and businesses enhance their cybersecurity defenses through a regional threat intelligence sharing platform to rapidly respond to indicators of compromise.

Background for SLTT Decision Makers

The intent and vision of this pilot project was to create a regional Information Sharing and Analysis Organization model to serve as an example for other cites or regions. The core initiative of the pilot is the mutual exchange of cyber threat intelligence (CTI) across private and public sectors while creating a collaborative real-time identification and analysis of cyber threat constraints. CTI sharing is widely believed to be the next logical step in the establishment of a national collective cyber defense strategy. Private sector participation is voluntary and public sector resources are limited thus creating connections between these groups foster greater access to CTI and thereby begin implementing security strategies faster. The final report highlights the tools, tactics and procedures used to create the regional cyber information sharing model.

PILOT PROJECT OVERVIEW

The pilot project was established to create the Internet Security Information Sharing Analysis Organization (IS-ISAO) to explore and evaluate the most effective methods for bi-lateral cybersecurity information sharing, focusing on regional information sharing, communications and outreach, training and education, research, and development for the improvement of SLTT government capabilities and capacity. The IS-ISAO developed the full capability to perform information sharing and analysis of cybersecurity threats, gather, and disseminate government and critical infrastructure information, for the purpose of:

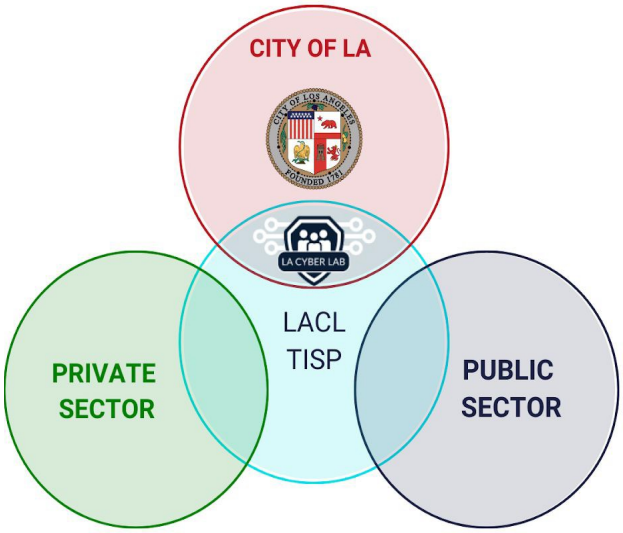
- Cyber threat analysis and information sharing
- Education/training/workforce development
- Technical research and development to support effective information sharing
- Share best practices IS-ISAO will promote and develop a collaboration

LACL THREAT INTELLIGENCE SHARING PLATFORM

Upon its launch, the LACL joined with the City to publish a daily threat report, documenting the “indicators of compromise” identified by the City each day, in hopes that the data would help businesses protect their systems from common attackers. In 2018, LACL was awarded a grant by CISA to expand this effort and establish itself as the nation’s first and only municipal-based Information Sharing and Analysis Organization (ISAO). LACL partnered with IBM and TruStar to develop the LACL Threat Intelligence Sharing Platform (TISP). The TISP allows for real-time automated threat indicator

sharing between the private and public sector. Features of the TISP include:

- **Automated Threat Sharing:** Using their existing security tools, partners can connect to the TISP to exchange threat data with one another, machine-to-machine, in real time. It enables members to leverage the insights and analysis developed by CISA, the City of LA, and other partners to protect their own systems.
- **Threat Intelligence Platform:** The TISP gives analysts and Threat Intelligence interface to pull in additional threat data sources, see trends, and perform research. The Threat Intelligence Platform can be used by organizations lacking the infrastructure for automated sharing.
- **Security Tool Integration:** The TISP includes pre-built applications that integrate with existing security tools, such as Security Information and Event Management systems.



RESOURCES FOR THE SLTT CYBERSECURITY COMMUNITY

The final report highlights the tools, tactics and procedures used to create a regional public private cyber information sharing model that others can replicate.

- Regional CTI Sharing Model - serve as an example for other cities or regions.
- Threat Intelligence Sharing - promote the bidirectional exchange of cybersecurity information to protect municipalities, SMBs, and organizations.
- Mobile Application Model – provide phishing analysis that connects SMB and individual citizens to business email compromise information.
- Connecting the Community - bring technology professionals, businesses and municipalities together to discuss cybersecurity related topics.
- Public-Private Partnerships - establish trust and confidence among technology professionals, business leaders, and government.
- Protecting Privacy Guidance - privacy consideration is a critical part of the information sharing process and is fundamental to the success of the ISAO in which information sharing is voluntary and based on trust.
- Documentation Development – examples of program design, policies and procedures, concept of operations, and operations manuals.

To download a PDF version of this report, visit www.cisa.gov/publication/internet-security-information-sharing-and-analysis-organization-pilot-report.

QUESTIONS?

For more information, email central@cisa.dhs.gov.