CITY OF SAN ANTONIO
INFORMATION TECHNOLOGY
SERVICES DEPARTMENT

ITSD Concept of Operations

Alamo Regional Operations Center (ARSOC)

July 19, 2022

Alamo Regional Operations Center (ARSOC)

Concept:

The ARSOC vision is centralized security operations providing real-time, collaborative, cyber-security information sharing among municipal and local government entities in the San Antonio Area. The ARSOC is a 24x7 collaborative ecosystem committed to providing operational and training environment where partners can come together to enhance the protection of each other's systems from threats. The ARSOC will focus on strategic and tactical approaches to collaborative defense using advanced and emerging technology, developing public-private partnerships in support of cyber security, collaborative skills development, and regular training exercises for regional municipal organizations. The ARSOC will allow the Alamo region to monitor, train, defend and respond together to cybersecurity threats facing the community and become the model for Collective Cyber Defense through Cyber Mutual Assistance (CMA). Additional partners being considered are CPS Energy, San Antonio Water System (SAWS), Bexar County, VIA Metropolitan Transit, Edwards Aquifer, River Authority, and Alamo Regional local governments.

Key functions include:

- COSA ITSD Security Operations
- COSA Service Desk Operations
- COSA Network Operations
- CPSE Cyber Intel Analysis
- CPSE Supervisory Control and Data Acquisition (SCADA) Lab & Training
- Joint ARSOC Operations Floor (multi-tenant)
- Joint ARSOC Training, Cyber Range and Conference Rooms
- Collaboration with Educational partners in the Alamo Region with internship opportunities

ARSOC value for the Cybersecurity Ecosystem in San Antonio and the Alamo Region

The ARSOC represents one of the most significant strategic assets and investments that City of San Antonio will make to support the growth of the regional cybersecurity ecosystem. The ARSOC will create a physical environment and virtual partnerships that bridge education, training, entrepreneurship, critical infrastructure defense and continuity of government operations. The establishment of the ARSOC signals San Antonio's dedicated focus to becoming a national leader in cybersecurity. The ARSOC name defined the true concept of support and is in keeping with the City of San Antonio's mindset that cyber security does not stop at the lines drawn on maps; what affects our surrounding communities affect the City of San Antonio. It is our belief that when our neighboring communities are protected, we are all better protected.

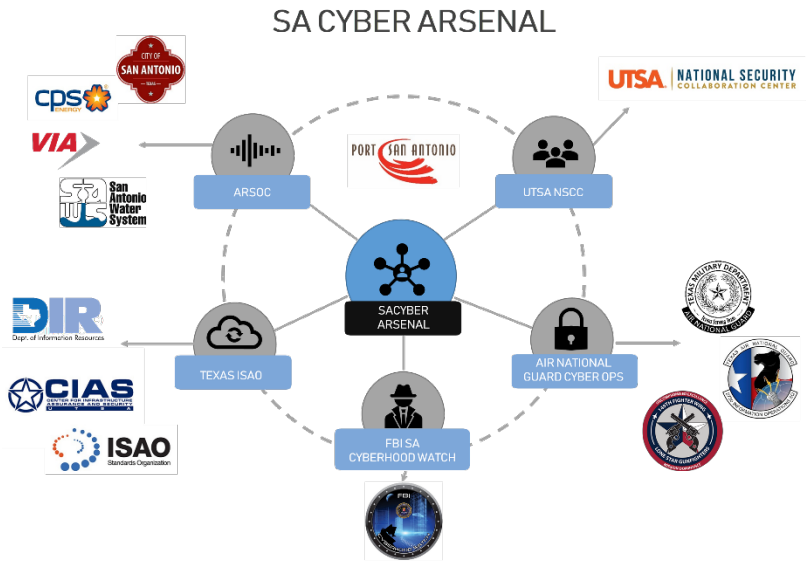
ARSOC Facility

A 20,168 square foot facility, located on San Antonio's Cyber Campus at Port San Antonio, adjacent to other critical assets and agencies that operate cyber and intelligence missions in support of national security. The integrated working and training facility will provide a unique environment that allows municipal agencies to share threat intelligence, work collaboratively to respond to threats, enhance training within their employee base, and simulate incidents based on real-time data. The collaborative operations center will create a rapid response team that supports ARSOC partners capability to respond to cyber threats.

Location Cluster Advantage

Port San Antonio is building an innovation campus that creates the brings additional value, resources and missions in an adjacent capacity to the ARSOC. Already home to 24th Air Force (Air Forces Cyber), and over a dozen major cyber operations and training facilities managed by private-sector companies, the campus allows for unique collaboration between government, industry and academia.

- The Port is building an Innovation Center that will house unique assets that can support the mission and growth of the ARSOC, including:
    - 2,000-seat technology arena
    - San Antonio Museum of Science and Technology
    - 30,000 sq ft Industry Showroom with advanced demonstration, training and prototyping capabilities
    - 40,000 sq ft office and lab area to support small companies, applied R&D and critical infrastructure testing environments
- Relevant Defense Industrial Base capabilities and testing facilities are located throughout the Port's 1,900 acre campus that understand electromagnetic hardening of control systems, offensive cyber threats and the application of artificial intelligence and machine learning security systems – all of which will work with the ARSOC and regional agencies.



Capabilities Located within the ARSOC

- City of San Antonio (COSA) Information Technology & Security Department (ITSD) Security Operations and Training
- ITSD Support operations
- SAPD Fusion Cyber
- Cyber & Supervisory Control and Data Acquisition (SCADA) Lab & Training Environment
- Partner Collaboration and Training
- Collaborative Vendor Training
- Cyber Range capability
- Regional Participant Cyber Exercises

Benefits / Business Case for COSA

- **Security & Resiliency**
  - Force-multiplier for security teams within the ARSOC partner agencies; including federal partners such as FBI, Secret Service, NSA, DoD, and regional private entities such as Chamber of Commerce and local educational institutions.
  - Internet log capturing and data analysis enrichment platform available to partners to create real-time threat intelligence and data sharing construct – creating increased situational awareness and operational metrics for the Alamo Region.
  - Pivotal partner for Texas State initiative to create Regional Security Network Centers as well as a regional Information Sharing and Analysis Organization (ISAO) partner for the Texas ISAO and National Cybersecurity Alliance.
  - Creation of a culture of Collaborative Cyber Defense through CMA that will become a statewide model for collaborative security operations.

- Alignment and operational intelligence support between the ARSOC and the City's Emergency Operations Center (EOC) and Southwest Texas Fusion Center.

- **Talent Development**
  - Real-time incident response, training and knowledge-building for multiple security teams across different municipal agencies, organizations and government partners.
  - Partnership opportunities with local colleges and universities for student training, lab usage and 'hands-on-keyboard' skills development.
- **Entrepreneurship**
  - Industrial Control Systems lab within the ARSOC will support municipal agencies' abilities to engage, test and prototype new technologies and solutions.
  - Shared, anonymized data allows new opportunities for emerging technology startups to showcase products and capabilities to municipal technology and security leaders.
- **Research & Development**
  - Joint partnerships with UTSA's National Security Collaboration Center (NSCC), Center for Cyber and Texas Department of Information Resources (DIR).
  - Data Analytics and Center for Infrastructure Assurance and Security (CIAS) will allow for talent recruitment, knowledge-sharing and applied research projects that support the operational success of the ARSOC.

Operational Goals:

1) Preventing cybersecurity incidents through proactive, operational monitoring, detection, and analysis of potential intrusions in real-time.
   a) Continuous threat analysis of collaborative environments.
   b) Leverage tools, buying power, and skills while maintaining regulatory segmentation.
   c) Network and host scanning for vulnerabilities.
   d) Historical trending on security-relevant consolidated data sources.
   e) Integrated and collective defense against stated threats.
2. Coordinating and integrating response to confirmed incidents, providing real-time situational awareness and reporting on cybersecurity status, incidents, and trends in adversary behavior to regional member organizations.
   a. Collaborative sharing of live events, indicators, and intelligence among partners.
   b. Countermeasure deployment coordination.
   c. Leverage shared operational resources as a force multiplier.
   d. Mentoring, enhanced training and cyber exercise environment.
   e. Integrated Cyber Intelligence Exchange with local, state and federal.
   f. Federated access (PIV-I/PIV/CAC) to appropriate systems.
   g. Integration with San Antonio Emergency Operations Center (EOC).
3. Integrated technical infrastructure and security procedures for partner collaboration.
   a. Facility and system certifications.

   b. Security policy and architecture consulting.
   c. Formalize cooperative training Cyber Exercise and preparedness programs.
4. Creating a security training ground for local talent through CivTechSA program, providing Cyber Range access for collaborative training in cyber defense.
   a. Shared Training of Alamo Regional Cyber Security partners' Team members where none exists today.
   b. Train K-12, collegiate, post-education, talents to hone skills in cyber security in real world situation and produce Turn-key and experienced "generational" Cyber Security workforce for The Alamo Region.
   c. Sharing information and showcasing cyber security tools and technology, its integration, capabilities and efficacy for our regional partners.
5. Modeled for Collective Cyber Defense through CMA, assisting partners, public and private entities in the Alamo Region.
   a. Readily provide aid to regional partners and community in cyber defense and mitigation efforts.
   b. Aiding the surrounding community and COSA partners make for a safer cyber ecosystem in which to operate and serve the residents in the Alamo Region.

Appendix A

Types of Agreements

1. **Subleasing Partnership** – Operational Partners cost associated
    a. Integrated Operations – Operations Floor access
        i. Integrated Operations is limited to Releasable information that does not affect individual operational requirements and regulatory restrictions. Mainly knowledge sharing of Cyber Security information.
    b. "Permanent Access" to facility with approved security/background checks.
    c. Cyber Range access, Exchange/sharing of information, Training, Assessments, IT Security Posture assessment/enhancements, Compliance/regulatory requirements/awareness/applications, System Configuration assistance, Tabletop exercise participation/involvement, Train each other.

2. **Participants** (Mutual Aid, ISAO model, no cost)

Cyber Range access, Exchange/sharing of information, Training, Assessments, IT Security Posture assessment/enhancements, Compliance/regulatory requirements/awareness/applications, System Configuration assistance, Tabletop exercise participation/involvement, Train each other.

    a. Temporary Duty at ARSOC (3-6 months 1-2 days/week)
        i. Support ARSOC Missions.
        ii. Non-integrated Operation
        iii. "Temporary Access" to facility
    b. Offsite
        i. Sharing information, Training, Mutual aid
    c. Must be approved by Plank-owners (COSA, CPS)