Community Security Best Practices - CSBP

Incorporating PSeMS, A Security Quality Management System

Designed for Public Safety and Critical Infrastructure Security Mitigation

Together, We Are A Global Force

This booklet is a preview guide to the Community Security Best Practice Security Manual, which is available to all member authorities.

PREVIEW GUIDE

Practice Principles:

- Lessons Learned Tactics
- Evidence Based Practices
- GAP Analysis Diagnostic Audit
- Quality Management Systems
- Training & Implementation
- Collaboration Strategy
- Communication Engagement

PREVENT - PROTECT - PREPARE - PURSUE

SEE SAY ACT For a Safer Community

COMMUNITY SECURITY BEST PRACTICES (CSBP)

The CSBP practices bring together the principles of Protective Security Management Systems (PSeMS) and the learnings from Project Griffin International (PGI), forming a methodology and approach that supports security resilience. Our CSBP observations and recommendations incorporated into this document provide insight based on evidence-based practices and lessons learned. Recommendations throughout this document are based on evidence best practices from our international counterparts involved in security. Including those from Canada, European Nations, the United Kingdom and the United States.

Today's cities, public transportation, mass-public environments, and other critical infrastructures need to be among the most forward-thinking and proactive to enable effective threat mitigation based on the continual threat of terrorism. Security and policing approaches for the protection of these environments is paramount. There is a public expectation of being safe and secure when in such environments. We approach these requirements with a proportionate risk perspective on prevention and protection that addresses terrorism and criminal activity using an approach which encompasses policing, security, and emergency response management.

We live in a complex and integrated world. The demand to communicate and keep the public informed at the same time enabling citizens and various stakeholders to be part of the community is essential. Providing timely and relevant information high-lighting matters of significance, great importance and life threatening situations allows for organizations to plan, prepare and act.

Quality security is a multi-agency requirement and encompasses community response. It cannot be limited to police and security personnel alone; it requires the cooperation and support of all stakeholders and importantly, the engagement and endorsement of senior staff within organizations. An organization's operational protocols should reinforce security with as much importance as that of, for example, customer service. Without such a commitment, the best possible protection can never be. For public safety and security to be genuinely effective, the commitment to integrate these practices throughout the environment is vital.

CONTENT

Security requires a holistic approach through evidenced based practices and technological capabilities throughout the community environment.

This effort must be embraced through a commitment of senior management and implemented throughout the organization.

INTERPORTPOLICE

Celebrating Over 50 Years of Global Service

WHAT WE DO!

Our mission is to provide leadership, assistance, and collaboration in security to address terrorism and transnational crime through expert advice, operational guidance, and training. Through the sharing of best practices focused on Prevention, Protection, and Preparedness, efforts towards aviation, maritime, and related transport and mass environments can assist in the reduction of their vulnerability to protect human life, the global supply chain, and critical infrastructure.

WHO WE WORK WITH!

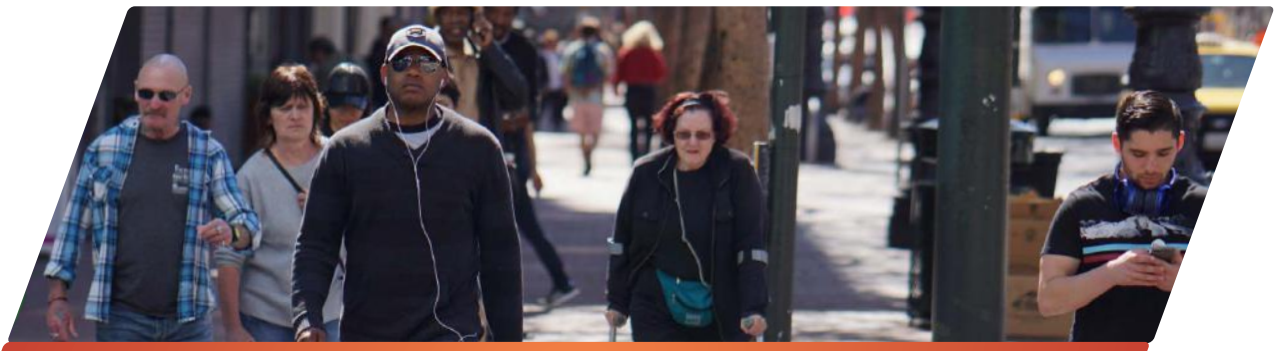
We endeavour to ensure that all authorities can benefit from the expertise and facilitation through assistance and training programmes. Our efforts include collaborative authority outcomes and a range of partners to assist in identifying risk and reducing vulnerability. Collaborative threat prevention and risk mitigation as a global team effort in addressing public safety and critical infrastructure for mass environments. We also bring together key partners in government, agencies of the United Nations, supporting organisations and appropriate businesses partners.

- Together, We Are a Global Force -

Objective

This Community Security Best Practice (CSBP) aspiration is to provide valuable guidance, tactics and technology solutions to the three areas of prevention, protection, and preparedness. An approach designed for those who have responsibility for the provision of safety and security of their organization. To be embraced by those who are accountable and responsible for the management of safety and security within public transportation, critical infrastructure, mass-public gatherings and every-day life. This document highlights protective measures to help mitigate risk within the environment through collaboration and stakeholder engagement, driven by director and senior-level leadership. The basis of this approach is that it takes a community to protect the environment. Ensuring there is a robust interface with the public and all stakeholders to the security of these environments is a crucial message of CSBP.

Community Intelligence is a two way street



Inclusive Measures

Security environments require affordable and comprehensive programmes that empower governments, regulatory authorities, and organisations to work together to identify and mitigate the impact of terrorism and other threats. This effort must include effective collaboration and ensure methods of communication are identified from BAU to crisis situations. This approach requires framework planning, regular integration based on identified responsibilities, and technologies that can support communication requirements.

SECURITY SCOPE REQUIREMENTS:

When evaluating public safety in a vulnerable environment it is important to integrate multiple requirements, e.g., policing, security, safety, customer service, emergency management, range of stakeholders, the likelihood of risk and threat, and so forth. The more comprehensive and planned these assessments are then the stronger the structure will be for providing coordinated management during a crisis, should such an event occur.

The content of the security requirements outcome will provide a diagnostic assessment based on existing strategy and operational conditions. This will enable improved risk assessment and help improve the response to any threat or crisis event. Evaluating your security approach often requires a new perspective. It is important not to accept the status quo of yesterday's practices and methods. Any review should be evidence-based and incorporate emerging threats and risk into a proportionate approach. The involvement of senior management and their endorsement of the approach is essential.

The purpose of an evaluation is to ensure and maintain the organisations effectiveness and resilience in its ability to respond to critical events.

Preventative & Operational Management

A public inquiry following a critical event will highlight deficiencies and may ask challenging questions. With the many incidents that have taken place if a jurisdiction has not addressed risk mitigation properly, there can be significant liabilities and repercussions.

Requirements to ensure security and public safety have changed with today's threats. Prevention and planning are essential and reaction to an incident requires a new approach that reflects and addresses the threat. Today's changing threat landscape needs to be considered to create a shift in practices and methods. Factors now need to include:

- Board Level accountability for security
- Enhanced stakeholder collaboration and communication
- Evidenced-based security
- More efficient business practices
- Threat assessment methodology integrated into BAU
- Empowering pro-active reporting
- Driving a more assurance-based system

SeeSayAct

The combination of the human element and technology can lead to effective security

Effective security requires a 'top-down' buy-in and the involvement of all the personnel

22 March 2016:
07:30: In my office working on a planned active shooter response training program for later that day; 07:58: 2 explosions;
08:05: smell of smoke, fire, and victims crying out;
08:30: our communications went out. We had to rely on runners and social media. We thought we were prepared, our planning, training, and communications were not sufficient.

Brussels International Airport Attack Lessons Learned - our team was in Brussels days after the attack being briefed by Belgium Federal Police

Commissioner Jean-Pierre Devos IPM
Brussels International Airport
Belgium Federal Police

From Day to Day Operations to Emergencies, Disaster and Crisis

Always in Touch

PREVENTATIVE measures are a key aspect of security; from the police, security personnel, government authorities, and other first responders. Connecting the environment's users to all the other stakeholders requires an integrated and collaborative approach. There is a need to communicate effectively by providing notices, alerts, daily operational communication requirements, etc.

Lessons learned have shown that it is essential to have well-established collaboration and communication protocols in place. Not only is this effective for day-to-day operations (BAU), but it becomes essential during an emergency and or crisis.

Today's collaboration and communication tools can bring a security environment together. This will often require an organization to look beyond traditional tools.

The security approach itself may need to change. It should incorporate the capabilities of emerging or new technologies and through proven approaches, integrate with lessons learned.

Essential collaboration

Situational Awareness

Good situational awareness in an environment will provide enhanced coordination. Having a common operating picture and being able to share that awareness accurately, effectively and in a timely manner is a key aspect to staying ahead operationally and in times of crisis. This includes an informed local population base or critical infrastructure personnel, tenants, vendors, and public.

Geo-location communication provides for accurate dissemination to inform and can further link to more comprehensive information in addition to collaborating effectively. Systems can be stand alone or integrated with various tools, such as computer-aided dispatching systems (CAD). The movement information should not be silo based, but have the capability to be disseminated as required internally and externally including concurrently through social-media; even pushing the data to the correct agency. Informed communication is critical in any operational environment.

Timely Information

Providing information based on where a user is currently located is a powerful tool to dispensing relevant and timely information. This is especially true for day to day management of information. Managing information is notoriously difficult operationally and becomes more difficult and stressful in an emergency or crisis because of the inherent uncertainty surrounding events.

Emergency & Crisis

When an emergency or crisis does occur, it is not the time for personnel to learn procedures, protocols, or the system. Providing for easy to use and effective communication platforms is vital to enable and engage real-time coordination. Comprehensive unified communication offers efficient management and less negative impact of an event. In a major crisis events mass evacuation and prolific social media communication are well documented. Proper interface and reaction to maintain control is critical. Single operational notifications through a common source is a preferred method of communication.

Reporting

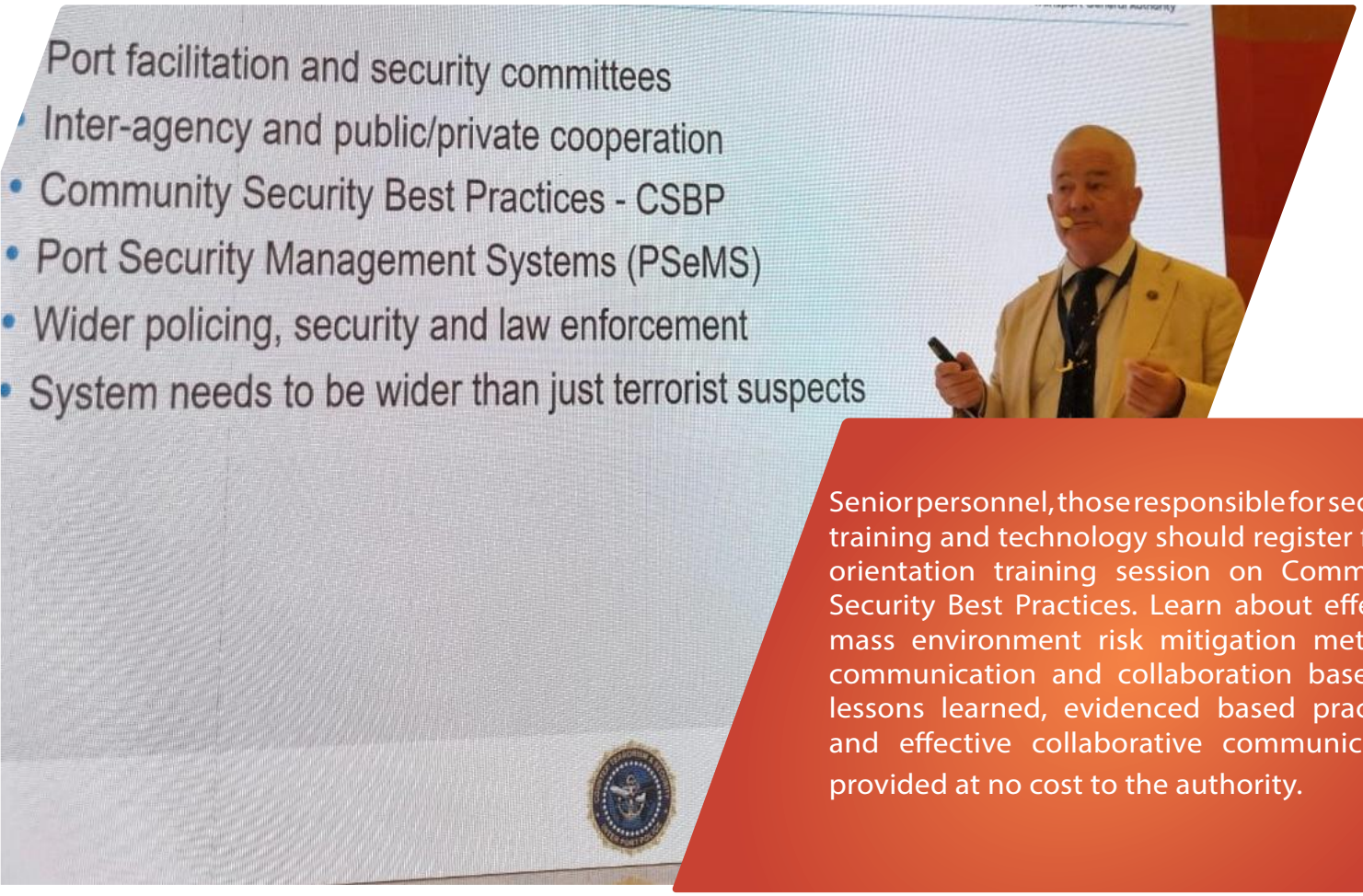
We advocate the use of using the public and environment personnel, regardless of who they work for, to assist in maintaining the environments safety and security. Having the ability of using their eyes and ears has proven to be extremely effective from the most routine to the most significant issues, including insider threat.

Operations

Adoption of an integrated and holistic communication and collaboration system has the ability to provide internal and external movement of information by an organization, one that is essential for operations and critical for emergencies. A silo approach is ineffective. Moving the right information to the right individual(s) internally and externally is an most efficient, offering unique insight, effective operations, and public safety.

Great things happen

when we work together



Senior personnel, those responsible for security, training and technology should register for an orientation training session on Community Security Best Practices. Learn about effective mass environment risk mitigation methods, communication and collaboration based on lessons learned, evidenced based practices, and effective collaborative communication; provided at no cost to the authority.

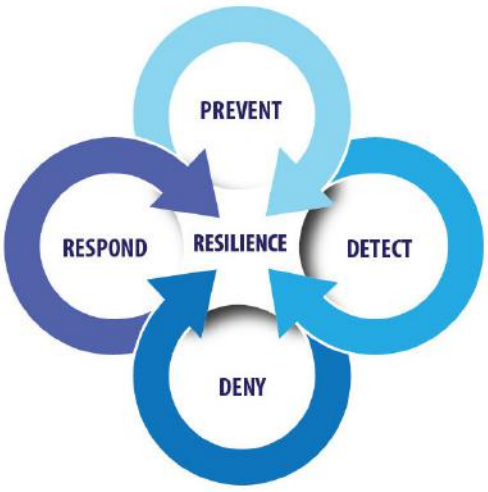
A security policy defines a code of best practices for staff, police, and security professionals to help with responsibilities and requirements. A good strategy also provides information for all staff as to how to help prevent, protect and prepare an organizations asset and ensure public safety; it provides guidelines as to acceptable (and unacceptable) practices and behaviour.

There is so much power and strength in the community, with the right engagement positive things can happen when we work together

Security plans should be kept secure but available to authorized access. Documentation needs to be reviewed periodically or where there is a change in policy and procedure, and at least every six months.

Senior management staff needs to be familiar with policy, process and procedures and support the development of a positive security culture. Security is everyone's responsibility. If management is not committed, there will be a gap in security assurance. One of the benefits of implementing PSeMS is the outcome of a positive security culture. PSeMS will compliment all processes and procedure, ensuring accountability and responsibility throughout the security process. Where possible, PSeMS integrated with existing organizational frameworks that are well established and operationally effective.

Resilience



- A key element of addressing today's threat environment is to incorporate practices that have been shown to have proven success in the past.
- A strategy that incorporates intelligence and evidenced based guidance can help to provide sustainable solutions.
- It is vital to incorporate a holistic plan that covers the requirements of the entire entity, can be proven to be effective operationally usable, and can be supported financially.

It Starts With A 60 Minute Training Session >

As part of the training process we introduce key aspects of threat awareness, collaboration, and communication

Neville Hay, Avsec PM, MSyl
Director of Training
E: neville.hay@interportpolice.org

Training Programs Include:

- Project Griffin's Train the Trainer (Operational Awareness)
- PSeMS Environment Implementation
- Risk Assessment & Verification Operations
- Environment Security Strategy
- Griffin on the Go (Operational Deterrence)
- Crowded Environment Communication Strategy

Our professional staff have many years of security, counterterrorism, and workforce optimization experience. We also teach globally through the UN and other programs.

They are available to train your staff to help you create enhanced security assurance for your organisation.

E: training@interportpolice.org

W: https://interportpolice.org/

Security Scope and Evaluation

When evaluating public safety and security within a critical environment, it is crucial to consider all stakeholders within that environment, e.g., police, security personnel, tenant organizations, fire service personnel, port authorities, etc. Ensuring collaboration between all such groups will help provide a robust structure facilitating a coordinated security management team and a more coordinated response to any security incident.

The Community Security Best Practice (CSBP) guidance provides a proven strategy based on the following three areas:

- Education
- Collaboration
- Communication

For a Safer Community

Start With: A Security Training Workshop

Register for an introductory workshop:

- Learn the basics of implementing PSeMS, a security management system, how it can assist your organisation, to provide security assurance and develop a strong security culture
- We provide an overview of how to implement effective communication and collaboration in mass environment. Keeping your organisation informed
- Once you have reviewed the CSBP preview guide and register for the free workshop we will get you started and provide additional information on any of our services

Target Audience

Command Law enforcement, Senior personnel and managers with security, safety, health and quality management responsibilities, maintenance, suppliers and service providers with security responsibilities, and regulators and legislators.

Upon Completion:

- A Project Griffin International certificate of completion will be issued for those attending the orientation.
- The CSBP-PSeMS Practice Guide and GAP Analysis will be made available to the authority.
- The authority will be issued one Atlas One Essential Environment License at no cost on-going. This will provide operational and emergency assistance for the public safety of a jurisdiction, offering multi-layered mass notification and geo-fenced notices and alert as the user approaches the designated area, as defined by the authority or user.

PSeMS: *An assurance system for your organisations security*

PSeMS provides a systematic approach to managing security risks incorporating security management into the daily activities of your organisation. It is a proactive approach for assessing and managing holistic security risks. The PSeMS framework and approach helps coordinate processes and procedures covering governance, legal requirements, operating procedures, delivery, monitoring, review, and audit to ensure effective oversight of security. PSeMS can help to identify and mitigate gaps in an organizations security and is a fundamental building block for effective management of security and risk mitigation. In simple terms, it is a framework and methodology for your organization's security assurance.

As with all management systems, PSeMS provides for goal-setting, performance measurement and planning. It focuses on maximising opportunities to continuously improve security and the system itself. It is not about implementing a new systems or process, but ensuring existing processes are coordinated to ensure a holistic approach to security.

PSeMS is designed for senior leadership teams and security managers. PSeMS can raise the profile and importance of security at all levels across your organisation. It establishes the need for senior management support, review and oversight promoting where necessary the need for security investment. Having an accountable manager at board level, your senior management teams will see the benefit of having security governed, resourced and managed to the needs of the organisation

PSeMS guidance does not replace existing systems such as those of quality management, safety management or ISO Standards but should be integrated into the fabric of the organisation as a gateway to other Industry Standards and regulatory frameworks, accreditation and certification schemes.

PSeMS protective principles apply to all applicable security domains such as information, physical, cyber, and personnel; and helps integrate all these domains.

PSeMS principles apply to all applicable security domains such as information, physical, cyber, and personnel; and helps integrate all these domains. The core principles are:

- An assurance system for an organizations security
- Provides the necessary organizational structure, accountabilities, and policies to ensure effective oversight
- Supports an organizations systematic approach to managing security risks incorporating security management
  into the daily activities of an organization.

We recognize that organizations can often have 'siloed' departmental structures leading to possessive ownership of issues and concerns that are not shared or dealt with for the benefit of the organization. The organization can then fail to identify all risks to the organization. Senior management can demonstrate a strong commitment to security but fail to resource security departments adequately. This can result in a 'security department' lacking the resource to sufficiently address emerging or new challenges with security requirements seen as a barrier to effective working unless staff awareness and training provided supports the organization's strategic objectives.

Andrew McClumpha
Head, Standards & Practices
E: andrew.mcclumpha@interportpolice.org

The Protective Security Management Systems [PSeMS] was the outcome of a multi-year program led by McClumpha Associates Limited working closely with senior representatives of the UK's Critical National Infrastructure [CNI]. The Port Security Management System is a derivative of the CPNI programme. We are pleased to welcome Andrew McClumpha as part of the InterPortPolice experts. PSeMS is a programme of the United Kingdom's National Security Protective Authority.

Practice Guide:

The CSBP/PSeMS Practice Guide is available at no cost. Senior and management authority officials are encourage to attend the 60 minute overview course for additional details.

The Practice Guide Chapters include:

- > Primary Considerations
- > Critical Infrastructure
- > Security Scope and Evaluation
- > Learning from History
- > Port Security Management Systems
- > Security Integration
- > Project Griffin International Community
- > Security Risk Planning
- > Intelligence
- > Joint Intelligence
- > Insider Threat
- > Communications
- > Media
- > Technology Systems
- > Closed Circuit Television
- > Crisis Response
- > Training and Exercising
- > Staff Requirements
- > Evidenced Based Practices
- > Register
- > Training and Services Provided
- > Portals and Communication
- > Evaluation, Review & Certification

PSeMS *Comprehensive Implementation Training Available*

The PSeMS five-day workshop will provide participants with a broad and detailed understanding of how to implement and maintain a Security Management System. The course provides a practical guide to the benefits of PSeMS derived from international best practice, extensive case studies, interactive sessions, and presentations. The training brings together the resources of the stakeholder community and includes, police, emergency services, local authorities, business, and private sector security industry and staff to make an overall safer community.

Objectives

At the end of the workshop participants will be able to:

- Explain what a Protective Security Management System (PSeMS) is
- Understand the benefits of PSeMS to the organisation
- Conduct a risk and vulnerability assessment and review processes to prioritise and manage security risks
- Design, plan, and implement a PSeMS applicable to your organisation. Assess, manage, and ensure stakeholder
- Implement measures to benchmark and assess the effectiveness
- Ensure continual security assurance and improvement
- Create a PSeMS Business Case
- Support and manage the change that a PSeMS can provide
- Explain the importance of creating a positive security culture
- Develop a PSeMS training and awareness provision

Environment Communication

We began our quest for effective environment communication in 2014 soon after the 2013 Los Angeles Airport (LAX) active shooter incident, we began a global incident learning process with authorities and technology experts in a quest to identify functional operational to crisis management communication and collaboration solutions. Systems that work in various conditions, provided timely trusted information, and will allow an authority to provide internal and external environment tools. We have combined this with our SeeSayAct.com programme for environment engagement, and are pleased to introduce an enterprise solution that meets our criteria and offers various levels of features starting at a basic but essential environment notification programme at no cost, a reduced cost Professional Plan to a fully integrated enterprise system.

An integrated safety and security communication Authority platform for essential communication

From customer support to essential solution requirements, Atlas One provides a unified communication platform that supports the principles of preventative, protective and preparedness, while keeping people safe. Forming a methodology and approach that encompasses security resilience . Whether your organization is an airport, seaport, transport, border guard, coast guard, or city environment, the unified system enables collaborative secure managed communications.

COMMAND AND CONTROL - Operational and incident management
Engage personnel, passengers, tenants, and surrounding environment parties in real-time. Respond effectively and efficiently with operational use that allows for readiness in escalating incidents. Place the authority in control of message and multi-media communications, allowing citizen engagement to various layers of environment personnel. Managing social media rumors to segregating information when directing personnel and tenants is critical.

SAVE VALUABLE TIME - Integrated Systems
The unified communication platform allows for integration with computer aided dispatch (CAD) and 911 systems. It provides interoperability with other agencies, and collaboration with stakeholders. In addition, there are opportunities to integrate with various audio and visual communication requirements, from the hearing impaired to managing emergency evacuation. In a crisis, time saves lives.

REDUCE LIABILITY - Keep the people in your environment informed
Send information and multi-media messaging based on multiple and layered geo-fenced area(s), such as a terminal gate(s), portions of a tarmac, terminal or platform, and other open, secured, and sterile zones. Messaging to internal channels allows for management of police and security, staff, tenants, other requirements, and through traditional social media channels.

SEE SAY ACT - Collect crowd sourced reports across your digital channels
Your employees, tenants and customers are the ultimate force multiplier. Mitigate your insider threat. Collect real-time crowd sourced reports from social media, mobile apps, and SMS. Share internally, or within your entire environment, and respond in real-time.

RELIABLE COMMUNICATION - Reduce the possibility of total communication failure
Documented crisis incidents have shown the vulnerability of radio and mobile phone circuit operability from being impaired to complete failure , yet communication such as social media has prevailed. The unified communication platform reduces the chances of communication collapse.

A JURISDICTION

AN AREA, BUILDING, or SUB LOCATION

CURRENT DASHBOARD FEATURES ARE CURRENTLY IN ENGLISH ONLY BUT BROADCASTING AND INTERFACING WITH THE ENGAGE COMMUNITY CAN BE IN ANY NATIVE LANGUAGE

Our Commitment to Making the World a Safer Place

All partner programs are through the Morrone 9/11 Center. Some programs may provide grants, scholarships, or referral fees to the 9/11 Center, a qualified 501c3 nonprofit. It is our goal to partner with government and other organizations where great value is brought forward in brining public safety to mass and critical infrastructure environments. Other offerings , features and capabilities may be available that are not included in our

Register: Change Your Mindset

Start the Environment Protection Review

Rethink security based on evidence-based practices and lessons learned:

1. Learn more about SeeSayAct.com
2. Learn more about the Atlas One collaborative software
3. Take the next step and dive into the Community Security Best Practice Guide; and GAP Analysis

INTERPORTPOLICE

W: https://interportpolice.org

E: info@interportpolice.org

IN COOPERATION WITH

MORRONE 9/11 CENTER

W: https://911center.org

E: info@911center.org

See Say Act.com and the PSeMS programs funding is partially assisted by the Morrone 9/11 Center for Counterterrorism and Security, a 501c3 chartered nonprofit. Your support and donations are appreciated.