STAFF REPORT FOR CALENDAR ITEM NO.: 15
FOR THE MEETING OF: March 10, 2016

TRANSBAY JOINT POWERS AUTHORITY

BRIEF DESCRIPTION:

Presentation of the Safety & Security Concept of Operations (ConOps) for the Transbay Transit Center Program (Program).

SUMMARY:

The ConOps is a comprehensive strategic document that identifies best practices and critical safety and security procedures to assist the TJPA in developing a safety and security program that promotes the safety and security of transit passengers, transit operators, tenants, employees, and members of the public using Program facilities. On May 8, 2014, the TJPA Board authorized the Executive Director to execute a Professional Services Agreement with Ross & Baruzzini to prepare the ConOps documentation.

Agencies such as the Metropolitan Transportation Commission, BART, AC Transit, San Francisco Municipal Transportation Agency (SFMTA), California Department of Transportation, San Francisco International Airport (SFO), United States Coast Guard, Federal Highway Administration California Division, and General Services Administration prepare ConOps to describe how security and other systems and procedures are expected to operate in their intended environments, as well as the training required to implement the ConOps.

Ross & Baruzzini previously prepared a ConOps for SFO and has extensive experience in safety and security planning and implementation, management services and emergency response planning for the Federal Transit Administration and transit agencies such as SFMTA, BART, AC Transit, Caltrain, Port Authority of New York and New Jersey, Northstar Corridor Rail Project, and Dallas Area Rapid Transit.

The ConOps for the Program provides both preventative strategies and response strategies to address threats and hazards at the Transit Center. It recommends security-based staffing levels and specific training, and exercises to be undertaken during normal operating conditions to provide the best opportunity to prevent, delay, and/or detect an undesirable event before it takes place. It identifies, among other things, recommended operational measures, procedures, and response plans in the event of a safety threat, such as a fire, medical emergency, or crime. It recommends a plan for coordination and cooperation among the TJPA, authorities having jurisdiction (e.g., San Francisco Police Department (SFPD), San Francisco Fire Department), transit agencies using the Transit Center, neighboring property owners, and other stakeholders. The ConOps also includes recommended audit, compliance, and quality assurance measures and implementation plans and will inform the maintenance and operations needs of the Transit Center.

The Master Lessee will be responsible for conducting facility operations in coordination with the TJPA's security staff to support safety and security operations. Recommendations regarding the Master Lessee's role and responsibilities with regard to the TJPA's safety and security program are discussed throughout the ConOps.

Implementing the ConOps recommendations should assist the TJPA with meeting federal, state, and local regulations that may impose safety and security requirements on the TJPA, and support the TJPA's application for designation and/or certification under the Support Anti-terrorism by Fostering

Effective Technologies Act of 2002 (the SAFETY Act), as well as applications for federal, state, and local funding to assist in implementation of safety and security measures for Program facilities. The ConOps documentation has been prepared to support the TJPA's application for SAFETY Act designation/ certification.

The ConOps documents are considered to be "living" documents: they should be periodically reviewed, including after incidents, and lessons-learned incorporated into updates. The ConOps is responsive to the phased design, construction, and occupancy schedule for the Program.

CONOPS PLAN OUTLINE:

The ConOps consists of the ConOps Plan, functional annexes, and support annexes. The ConOps Plan describes the safety and security procedures for daily operations of Program facilities and comprises the following sections:

Section 1.1 Safety & Security Mission Statement – *The Transbay Joint Powers Authority (TJPA) has an enterprise level commitment to providing safe and secure facility and transportation services to the Bay Area and the State of California, while creating a welcoming and pleasant environment for the users of the Transit Center. The Transbay Security Program will provide world class integrated, comprehensive, and balanced risk assessment, prevention, detection, communication, management, and mitigation capability to safeguard Transbay personnel, passengers, guests, and property through coordination with federal, state, and local emergency responders and authorities having jurisdiction, transit agencies and tenants, and surrounding property owners*.

Section 1.2 Security Governance & Cooperation Plan – Identifies recommended formal organization and procedures for governance and cooperation between the TJPA and stakeholders to support the TJPA in discharging its safety and security mission. Recommends a clear and definitive master plan for stakeholder engagements, systems interoperability, staffing and jurisdictional responsibilities, physical and intellectual resource and information sharing, training, and joint exercises, and includes recommended scope and content for agreements between the TJPA and third party entities to clearly delineate duties, roles, obligations, and responsibilities.

Section 1.3 Strategic Policing Coordination Plan – Identifies the recommended approach to policing and security of the Transit Center including use of TJPA-directed/deployed security forces, the SFPD, transit agency law enforcement, and transit agency security personnel and programs. Developed in coordination with the SFPD and based on the best practices of peer facilities and rail and bus transit agencies, Section 1.3 provides a recommended framework for the TJPA to accomplish the following: establish agreements for the coordination of law enforcement and non-law enforcement safety and security operations throughout Transit Center; operate effectively within and in coordination with the jurisdictional coverage of multiple police agencies; establish procedures and protocols to effectively and efficiently respond to all-hazards (man-made, natural, technological and cyber) events in coordination with multiple agencies; leverage Transit Center security technology as a force multiplier and provide situational awareness and a common operating picture for normal and emergency conditions; and finalize procedures to support operational safety and security.

Section 1.4 Security Operations Center (SOC)/Train Operations Center (TOC) Stakeholder Coordination & Liaison Plan – Provides a framework for SOC operations, structure and organization, objectives, and priorities. Recommends formal procedures for coordinating SOC and TOC operations during normal and emergency operations. Includes scenarios that recommend a systematic process for SOC operations during events that require coordination with stakeholders and programs, which include transit agencies; retailers; adjacent property owners; governmental entities; park management entities; vehicle/cargo/mail screening programs; trusted access programs for

persons, vehicles, parcels, baggage, and cargo; and various disaster and emergency management response plans.

Section 1.5 Core Business Practices for Safety & Security – Supports day-to-day operations, policing, and incident response; provides a comprehensive operational framework and approach to staffing, programs, and project requirements to support effective and efficient deployment of resources; and includes TJPA organizational planning and a structure for security management and key stakeholder agreements.

Section 1.6 Local Law Enforcement & Fire/Life/Safety Plans – Summarizes expected local, regional, and state plans administered by external response agencies, which may be activated during an incident occurring at or near the Transit Center and describes the TJPA's understanding of external response agency plans that are intended to address not only exceptional events but also pre-event intelligence sharing, general crime deterrence, day-to-day policing, and community relationships provided by the law enforcement community. Section 1.6 was developed in coordination with SFPD and is based on the best practices of peer facilities and rail and bus transit agencies.

Section 2.1 Site-Wide Communications Plan – Provides recommended operational measures, policies, procedures, use of system technologies, and decision support templates for site-wide communications. The communications protocols address site-wide communications as well as the engagement of city and state emergency response agencies for local and regional event management.

Section 2.2 Rail/Bus Transit Interactions & Communications Protocols – Recommends operational measures, policies, procedures, use of system technologies, and decision support templates to support rail and bus interactions, protocols, and communications with transit stakeholders.

Section 3.1 Operational Measures – Recommends operational measures, policies, procedures, use of system technologies, and decision support templates to address roles and responsibilities and communications plans for incident response and incident management. Provides a strategic approach to policing and security of the Transit Center and its related facilities that includes the use of TJPA-directed/deployed security forces, local law enforcement, and transit operator security personnel and programs. Addresses site-wide communications, technology systems, resource planning, such as recommended staffing levels, and training, with specific focus on collaboration between the Master Lessee and TJPA security personnel to maintain an appropriate security and response posture and to support emergency response operations.

Section 3.2 Technology ConOps & Protocols – Provides descriptions of how the Transit Center technology systems should operate and interact with users and external interfaces under a given set of circumstances. Scenarios describe how various Program technologies function and interact. Each scenario describes a sequence of events, specifies the triggers for each sequence, describes the activities carried out by the user of the technology system and who performs the response steps, and provides details regarding when and to whom communications should occur and the information to be communicated. Includes templates for operational scenarios for both policing and incident management using technologies in the Transit Center and how and when the system of technologies should operate and interact with security personnel and associated stakeholders under different circumstances.

Section 3.3 Protective Design Elements – Provides an overview of the protective design elements (PDEs) integrated into the Transit Center design and related facilities in response to the TJPA's Risk and Vulnerability Assessment and Design Guidance Criteria. Includes discussions on the various types of PDEs implemented, their location, their basic operation, and how and when these elements may be activated during an incident occurring within the Transit Center security domain.

Section 3.4 Vehicle, Cargo & Mail Screening Plan – Provides Transit Center's mail room staff, loading dock staff, supervisors, and security staff and managers with a recommended framework for understanding and mitigating risks associated with various types of delivery streams. Identifies the most likely types of chemical, biological, radiological, and nuclear (CBRN) threats. Identifies appropriate screening technologies, facilities, and protocols and compares the efficacy, efficiency, and economics of alternative inspection and mail screening technologies, facilities, and processes. Defines an efficient workflow for delivery inspection, screening and sorting. Provides identification tools for suspicious mail and packages and strategies for contamination reduction. Identifies appropriate training for loading dock and mail room personnel. Provides suspicious substance-specific incident response procedures. Defines internal and external communications procedures.
Section 4.0 Plan Initiation, Maintenance & Change Management – Provides a recommended plan of action for initiating, maintaining, and managing changes to the ConOps.

The following functional annexes (FA) provide operational procedures for specific hazards and/or incidents:

FA 1.0 Emergency Operations Plan – FA 1.0 provides all-hazards response procedures based on principles set forth in the National Response Framework, National Infrastructure Protection Plan, and the National Incident Management System (NIMS)/Incident Command System (ICS). FA 1.0 includes an emergency response concept of operations and procedures for activation, direction and control, communication and notifications, situational awareness, logistics, and external collaboration in the context of ICS.

FA 1.1 Policies & Procedures for Incident Action Plans – FA 1.1 expands on tactical implementation of the ICS and provides field-level guidelines for the TJPA management level response operations.

FA 1.2 CBRN Detection, Mitigation, and Response Plan – FA 1.2 provides incident-specific procedures to support detection, mitigation, and response to a CBRN incident.

FA 1.3 Emergency Evacuation/Shelter-in-Place Management Plans – FA 1.3 serves as an initial evacuation and shelter-in-place management plan. FA 1.3 has been developed in the context of ICS and City of San Francisco and State of California emergency management guidelines, using standards such as those promulgated by the Occupational Safety and Health Administration.

FA 2.0 Facility Operations Security Guidance Document – FA 2.0 provides day-to-day operational security procedures based on internal capabilities. FA 2.0 addresses roles and responsibilities of the TJPA security management staff and contract security and provides clear delineation of responsibilities of stakeholders including bus and transit agencies, tenants, and external stakeholders.

FA 2.1 Post-Construction Retail Tenant Security Plan – FA 2.1 provides specific best practices to address the security and public safety needs and capabilities of retail and commercial tenants. FA 2.1 addresses the interfaces, capabilities, and responsibilities expected from tenants with respect to security within their lease areas and within public areas of the Transit Center.

FA 2.2 Park Security Protocols – FA 2.2 focuses specifically on parks under the TJPA's jurisdiction and includes security protocols for special events and venue operations, hours of operation, and pedestrian bridges, vertical transportation, and connections to adjoining properties. FA 2.2 is intended to be used by TJPA management, the Master Lessee, and the security team to develop and implement a park/green area rules and regulations policy that will foster a safe and secure environment for the public within these areas.

FA 3.0 Trusted Access Program – FA 3.0 provides protocols and operational measures to be implemented by the TJPA and Master Lessee to allow controlled access to pre-screened employees, tenant personnel, vendors, vehicles, parcels, baggage, and cargo. Measures defined in FA 3.0 include pre-screening for employees, background investigation, and identity authentication badging.

The following support annexes (SA) contain procedures and guidelines to either support response operations or to maintain effective emergency preparedness, safety, and security:

SA 1.0 Staffing Plan – SA 1.0 provides TJPA with staffing recommendations required to support the phased implementation of security operations at the Transit Center.

SA 2.0 Media Response Plan – SA 2.0 defines the role of the TJPA Public Information Officer, using ICS principles, and provides scripted messages and agency contact information to allow expedited media releases and public information. SA 2.0 also provides procedures for and parameters under which TJPA will participate with other agencies in a Joint Information Center (JIC) as an integral function of the ICS and the NIMS.

SA 3.0 Multi-Year Training and Exercise Plan – SA 3.0 provides recommendations for the frequency of training and exercises focusing on emergency response, safety, security operations. SA 3.0 provides a schedule for training and exercises, information regarding exercise types and duration, and suggested scenarios focusing on developing and maintaining staff competency of the Transit Center and plans and procedures to which participants may be assigned. SA 3.0 is written in compliance with the Homeland Security Exercise and Evaluation Program.

SA 4.0 Audit, Enforcement, and Quality Control Plan – SA 4.0 provides baseline and ongoing quality control parameters as well as audit and enforcement procedures to guide the security team and Master Lessee during the hiring, initiation, and management of personnel and in monitoring tenant compliance with lease agreements. SA 4.0 will be used to maintain quality in the conduct of day-to-day tasks and procedures and to ensure compliance with the ConOps and other requirements as defined by the TJPA. SA 4.0 identifies personnel responsibilities, audit schedules, means to evaluate results, and a methodology to correct deficiencies.

RECOMMENDATION:

Information only.

Safety and Security Concept of Operations (ConOps) Overview

March 10, 2016

Transbay Transit Center

TJPA

Transbay Transit Center

Agenda

- Overview
- Documents
- Organization
- Conclusion

Transbay Transit Center

ConOps Overview

- The Safety and Security ConOps is a comprehensive strategic document that addresses the process and strategy involved in preparing for, preventing, and mitigating against the impacts of threats and hazards affecting the Transit Center.

- In developing its strategy, the TJPA identified and analyzed potential threats and hazards and how they would likely affect daily operations at the Transit Center.

- The ConOps recommends best practices to be used by TJPA's security staff in developing detailed protocols and procedures for the safe and secure operation of the Transit Center and its related facilities.

ConOps Overview

- ConOps describe how security and other systems and procedures are expected to operate in their intended environments and the training required to implement the ConOps.
- The Master Lessee will be an integral member of Transit Center Security team, responsible for conducting facility operations in coordination with the TJPA's security staff .
- ConOps are widely used by federal, state and local agencies, institutions of higher education, the military, and transportation and transit agencies, including SFO, BART, SFMTA, and MTC.

Transbay Transit Center

ConOps Overview

The ConOps is designed to ensure the safety and security of the passengers, employees, transit operators, tenants, retailers, visitors, and other members of the public using the Program facilities.

ConOps address protective strategies that cannot be accomplished by physical, structural, or technological design elements in a built environment, including:

- **Implementing security management programs**
- **Organizing, training and implementing emergency management**
- **Leveraging safety and security technology**
- **Situational Awareness**

ConOps Documents

The ConOps is based on the Department of Homeland Security's National Incident Management System (NIMS) and National Infrastructure Protection Plan (NIPP).

- **Supports day-to-day operations**
- **Provides staffing plans, policing, and incident response**
- **Provides a comprehensive operational framework**
- **Provides an approach to staffing, programs, and project requirements to support effective and efficient deployment of resources**

ConOps Organization

- ConOps Plan – Provides strategic framework
- Functional Annexes – Provide function and/or hazard/threat-specific procedures
- Support Annexes – Provide maintenance procedures and augment operational procedures

Transbay Transit Center

ConOps Organization

ConOps Plan

Section 1.1 Safety & Security Mission Statement
Section 1.2 Security Governance & Cooperation Plan
Section 1.3 Strategic Policing Coordination Plan
Section 1.4 SOC/TOC Stakeholder Coordination & Liaison Plan
Section 1.5 Core Business Practices for Safety & Security
Section 1.6 Local Law Enforcement & Fire/Life/Safety Plans
Section 2.1 Site-Wide Communications Plan
Section 2.2 Rail/Bus Transit Interactions & Communications Protocols
Section 3.1 Operational Measures
Section 3.2 Technology ConOps & Protocols
Section 3.3 Protective Design Elements
Section 3.4 Vehicle, Cargo & Mail Screening Plan
Section 4.0 Plan Implementation, Maintenance & Change Management

Transbay Transit Center

ConOps Organization

Functional Annexes (FA)

FA 1.0 Emergency Operations Plan

FA 1.1 Incident Action Planning Guide

FA 1.2 CBRN Detection, Mitigation & Response Plan

FA 1.3 Evacuation/Shelter-in-Place Plan

FA 2.0 Operational Security Plan

FA 2.1 Retail Tenant Security Plan

FA 2.2 Park Security Protocols

FA 3.0 Trusted Access Program

Support Annexes (SA)

SA 1.0 Public Safety & Security Staffing Plan

SA 2.0 Media Response Plan

SA 3.0 Training & Exercise Plan

SA 4.0 Audit, Compliance & Quality Control Plan

Transbay Transit Center

ConOps Conclusion

When implemented, ConOps will support:

- **Business continuity planning for managing security, transit, retail and the facility including the park, and events**
- **TJPA application for Safety Act Designation.**