Bay Area UASI Management Team
Cyber Resilience Work Group
2020 Annual Plan

The Cyber Resilience Work Group is co-chaired by Mikyung Kim-Molina of the Bay Area UASI Management Team and Alison Yakabe of the Northern California Regional Intelligence Center (NCRIC). The Chairperson is responsible for developing meeting agendas, scheduling and facilitating regular meetings, and distributing meeting summaries to workgroup members.

The Cyber Resilience Work Group supports the following Bay Area UASI Goals:

#	Supported Bay Area UASI Goals
3	Enhance Cybersecurity

I. 2020 Regional Project Oversight

Consistent with the ongoing purpose as stated in the Cyber Resilience Work Group Charter, the work group will oversee the following projects:

- Cybersecurity Incident Response Framework Planning Project
- Cyber Tiered Training Project
- **National Priority Projects:** The Work Group will provide oversight and input to relevant projects within the National Priority areas as defined by the Department of Homeland Security in the UASI Notice of Funding Opportunity.

II. Member Roles and Responsibilities

Members of the work group are expected to attend scheduled work group meetings in person or via teleconference if necessary for the purpose of:

- Providing subject matter expertise and jurisdictional perspectives to the oversight of applicable projects
- Offering input to the work group and any active subcommittees to ensure relevant and quality outcomes of all projects
- Participating in the review of draft and final project deliverables
- Engaging in current regional collaboration efforts and reporting updates to their leadership.

The Cyber Resilience Work Group is scheduled to meet four times during 2020. Each meeting will last no more than 2 hours. Additional correspondence to work group members will be conducted via email from the Chairperson. Work group members are encouraged to participate in regional workshops, relevant trainings, and other events coordinated by this work group and its subcommittees. At a minimum, work group members should coordinate appropriate event participation by staff within their jurisdiction.

III. 2020 Active Subcommittees

Below are the current subcommittees which will report to the Cyber Resilience Work Group throughout 2020. Other subcommittees may stand up as needs arise.

Cyber Incident Response Framework Planning Subcommittee
This subcommittee is led by Mikyung Kim-Molina and will oversee the Cyber Incident Response Framework Planning Project.

Cybersecurity Training Program Subcommittee
This subcommittee is led by Mikyung Kim-Molina and will oversee the Cyber Tiered Training Project.

IV. Subcommittee Roles and Responsibilities

Each Cyber Resilience Work Group subcommittee will provide project guidance, oversight and stakeholder

representation in the development of the subcommittee's assigned projects.
Subcommittee members are expected to:

- Attend scheduled subcommittee meetings and respond to subcommittee correspondence
- Confirm project goals add value for the majority of Bay Area UASI jurisdictions
- Confirm the documented scope of work meets the goals of each project
- Oversee the progress of the relevant project and provide status updates to other UASI workgroups, the UASI Approval Authority, and other stakeholder groups as appropriate.
- Review draft project deliverables and provide input to ensure quality outcomes.
- Participate in planning workshops and other relevant project tasks by attending scheduled meetings and/or coordinating appropriate attendance from their jurisdiction.

V. Work Group Focus Areas

The following are proposed efforts and focus areas for the Cyber Resilience Work Group in 2020 and future years:

- Continue to maintain and cultivate stakeholder partnerships at the local, regional, state and federal levels
- Cross collaboration with states and jurisdictions outside of the UASI footprint (e.g., Nevada, Los Angeles, San Diego, NY)
- Exploring cybersecurity mentorship or apprenticeship programs to help leverage cybersecurity talent and resources for the region
- Researching cyber readiness gaps/needs and developing a regional response framework
- Understanding cybersecurity on critical infrastructure and industrial control systems (e.g., operational technology)
- Hosting facilitated walk-throughs of evaluation toolkits (e.g., NIST Framework)
- Participating in TTX or full-scale cyber resilience exercises
- Exploring the advantages of Artificial Intelligence (AI) and machine learning technologies
- Exploring Denial of Service attacks and identifying approaches to increase resilience to Denial of Service attacks
- Developing consolidated lists/calendars of cybersecurity-related meetings and events (e.g., MISAC, CCISDA)
- Exploring a mentorship program or other approaches to ensure learnings from UASI-hosted trainings live on in local jurisdictions
- Exploring the development of a regional Security Operations Center (SOC)
- Enhancing regional Cyber Incident Response capabilities through services or task force development
- Explore the development of MOU data sharing and mutual aid templates