CYBERSECURITY ANNEX

INTRODUCTION

This Annex to the Kern County Operational Area (OA) Emergency Operations Plan describes the strategic response of Kern County Information Technology Services (ITS) to oversee and coordinate the County's activities due to an actual or potential cyber-related incident.

Due to the unique challenges posed by a potential or actual cybersecurity incident, the responsibility for preventing, mitigating, and responding to such an incident is managed by County ITS and not through the EOC via its SEMS functions. If there are significant operational impacts to County departments or cascading impacts to the well-being of its constituents, the Kern EOC may be activated and those response efforts would be coordinated as needed by the EOC Director in liaison with ITS.

This Annex, therefore, is uniquely oriented to the Cybersecurity function and may not follow the format of other Kern EOP Annexes.

County entity which supports this Function:

- *Information Technology Services*
    - Coordinates with supporting stakeholders, state and local officials, and County partners regarding actual or potential cyber-related incident.
    - Responds to, mitigates the impact of, and coordinates the recovery from a cyber-incident, including use of the following strategies:
        - Planning
        - Risk management
        - Threat and vulnerability identification
        - Information security
        - Direction, control and coordination
        - Communications and reporting
        - Resource management.

PURPOSE

The Cybersecurity Annex is an essential element of the Kern County Emergency Operations Plan (EOP), which establishes an emergency management organization and defines the Kern OA EOC functional responsibilities in response to an emergency event. The Cybersecurity function described in this Annex is responsible for and expected to develop, implement, and test policies and Standard Operating Procedures (SOPs) that ensure necessary preparedness capabilities.

This document:

- Provides a basis for cooperation across agencies before, during and after a cyber-related emergency or disaster affecting, or having the potential to affect, the County or jurisdictions within the Kern OA.
- Describes the Kern OA functional responsibilities as required by the California Emergency Plan.

SCOPE

The Cybersecurity Annex of the EOP supports but does not supersede established protocols for dealing with day-to-day emergencies. It places emphasis on the unusual and unique emergency conditions that may require coordination and cooperation across agencies in response to a cyber emergency or disaster. The framework will ensure the incident involving critical infrastructure, technology emergencies, or other emergencies with impact to information technology capabilities is secure and protects the privacy of Kern County data. The framework will also utilize industry practices of NIST 800-61 Incident Response Plan to incorporate a standard approach to respond to and report the incident.

GOALS AND OBJECTIVES

The top priority of ITS regarding this Annex is to minimize cyber-disruption of County operations and the potential for cascading impacts upon lives, property and the environment.

The Information Security Office of ITS:

- Provides input to the EOC Director to mitigate operational impacts, as warranted.
- Establishes and maintains the Incident Response Team to detect, report, and respond to cyber incidents.
- Establishes information sharing in a way that protects data privacy, confidentiality, and sensitivity.
    - Coordinates with impacted stakeholders to include gathering and coordination of status reports ensuring compliance with state and local laws, schedules and communicates with outside partners, and identifies mission readiness.
    - Conducts briefings and shares information with affected stake holders;
    - Provides support to law enforcement agencies for criminal investigations as needed;
    - Provides recurring reporting to meet state and local reporting and promote awareness.
- Oversees the implementation of ongoing mitigation steps against a cyber incident, including:
    - Ensuring recurring data backups,
    - Maintaining awareness and training for users,
    - Performing security reviews for compliance,
    - Continuously reviewing policies and procedures.
- Responds to requests for cyber related assistance from Kern County cities and Special Districts, as indicated.

CONCEPT OF OPERATIONS

ITS will activate its resources as needed and as the incident dictates, for situational awareness of the incident and to oversee response strategies.

- *Whenever this Annex is activated, personnel are required to initiate and maintain Activity Logs in WebEOC (or hard copy ICS Form 214) to document their actions to facilitate and support cost recovery. (See Basic Plan for hard copy)*
- *Refer to the Kern County Incident Response Plan for further steps on identifying, responding, reporting, and mitigation to the incident.*
- *The Kern County Incident Response Plan incorporates the framework of NIST 800-63 and California Joint Cyber Incident Response Guide.*

Preparedness

- Review the EOP, applicable department plans, Standard Operating Procedures and the materials contained in this Annex and maintain familiarity with the roles and responsibilities of the function.

Initial Response

- Activate personnel as appropriate and brief subordinates.
- Provide information as appropriate to the EOC Director, to assist in development of emergency response strategies to operational impacts.
- Ensure all staff maintain required records including ICS Form 214 as well as all other documentation to support disaster assistance cost recovery, should the cyber event cascade into a disaster which is eligible for cost recovery.

Extended Duration

- Maintain situational awareness and adjust objectives as appropriate.
- Plan for functional relief and staffing schedule.
- Continue to participate in regular briefings and provide input to the EOC for its development and implementation of an EOC Incident Action Plan, as needed.
- Based on the situation as known or forecasted, determine likely future needs.
- Track and document all activities, costs and decisions for disaster claims and assistance applications.

NOTE: To obtain State or Federal reimbursement of disaster related costs, the first step begins with a Proclamation of a Local Emergency at the County level. Incidents which could potentially rise to this level should be communicated at the earliest opportunity to the EOC Director or the Emergency Services Manager. All personnel and incident related costs must be thoroughly documented. Further information on Emergency Proclamations is found in the EOC Procedures of the EOP.

Deactivation

- Authorize deactivation of organizational elements when no longer required.
- Ensure that any open actions are completed or transferred to other staff as appropriate.
- Submit documentation of all costs incurred to the EOC's Finance/Admin Section.

- Ensure completion of all required forms, reports and logs and submit to the EOC's Plan/Intel Section Documentation Unit.
- Provide input to the After-Action Report and Corrective Action Plan.

Recovery

- Revise and update emergency plans and procedures to reflect lessons learned from the emergency.
- Implement any assigned corrective actions.

ORGANIZATIONAL ROLES AND ASSIGNMENT OF RESPONSIBILITIES

Local Level (Kern County)

ITS manages the allocation of appropriate resources in response to incidents in the unincorporated areas of the county. If the emergency event occurs in another jurisdiction (e.g., city or special district) the affected jurisdiction has primary responsibility and will activate its own emergency management response as feasible.

Operational Area Level

Kern County and its political subdivisions become the Kern Operational Area (OA) for emergency response purposes during multi-agency disaster events, or as needed to support another jurisdiction within the Operational Area. ITS has overall responsibility for supporting mutual aid requests for resources under the jurisdiction of Kern County. Further, ITS will respond to requests for assistance from Kern County cities and/or Special Districts regarding cyber security issues, as needed.

INFORMATION COLLECTION AND DISSEMINATION

Briefings will be established with the EOC and applicable stakeholders of the incident's status and mitigations during the incident. An after-action report will be provided once the incident is complete. All information of the incident will be sensitive information and provided on a need-to-know basis to recipients. The EOC may use normal communication established through the WebEOC for other County business coordination.

ANNEX DEVELOPMENT AND MAINTENANCE

This document is an Annex to the Kern County Operational Area Emergency Operations Plan. As such, the policies, procedures, and practices outlined in the Kern County EOP govern this Annex. OES coordinates the maintenance and update of this Annex as needed. Record of changes, approval, and dissemination of the Kern County EOP also apply to this Annex.

FUNCTIONAL CHECKLIST

The tactical actions which support the Cybersecurity function are maintained by ITS, are limited in distribution due to their confidentiality, and are therefore not included in this Annex.