Annex O
State Emergency Function (SEF) # 15
INFORMATION TECHNOLOGY

LEAD AGENCY: Department of Personnel/Division of Information Technologies

SUPPORTING AGENCIES: All Agencies

I. PURPOSE

The purpose of this SEF is to collect process and disseminate information about information security and to coordinate the overall activities of a state response to mitigate information security risk.

II. SCOPE

The scope of this annex is to describe the overall operational and information activities of a state response to an information security emergency. Activities will take place at the Information Security Operations Center (ISOC), and in the field. SEF #15 activities include the following functions:

A. Planning Support - assess and consolidate information to support the action planning process at the ISOC and in the field.

B. Displays - to maintain displays of pertinent information by using computer system displays, maps boards, charts, status boards, etc.

C. Information Processing - to collect and process information from local jurisdictions, state SEFs, and other sources, process that information and disseminate it for use by response operations, and provide it as input for reports, briefings, displays, public information activities and plans and to maintain a permanent log of events and activities.

D. Reports - to consolidate information into reports and other materials describing and documenting overall response activities and keeping local, state and federal officials informed of the situation.

E. Public Information - To assure that the public is given appropriate information to deal with the emergency through SEF #12, Public Information (see Annex L) and the use of EAS, through SEF #2, Communications and Warning (see annex B).

III. SITUATION

An information security event usually results from man made technological cyber attack that produces damage and results in a large number of requests for services to mitigate the cyber attack. The state, when notified of an emergency situation at the state level, will monitor the situation and provide assistance as resourced.

IV. PLANNING ASSUMPTIONS

A. In order to identify response requirements of the emergency, there will be an immediate and continuous demand for information on the incident; its impact, magnitude and damages.

B. There will be a need for public information/instruction in all types of incidents.

C. The state agencies affected will be the immediate source of vital information regarding damage and initial response needs.

D. There may be delays in establishing full operational capability. Communications and network availability may be impacted depending on the type and severity of attack.

E. Situation/impact/damage assessment activities may be restricted by communications problems and other environmental factors and may cause cascading events.

V. CONCEPT OF OPERATIONS

A. General

1. In response to an incident, state agencies involved in the response will assess the situation to identify needs and requirements. These assessments require:

   a) Provide a gross assessment of event impacts including the identification of the network segment, type and severity of critical assets impacted.

   b) Determine the information needs of the agencies impacted by the incident(s).

   c) Determine the status of operational facilities used to mitigate the attacks including in house network operations and outsourced information security functions.

   d) Determine if the incident could be a terrorist action and respond accordingly.

2. In the initial period of an incident, the main avenue for the collection of incident information will primarily be from the impacted agencies. This information will be relayed to the ISOC through whatever means available, primary e-mail secondary telephone. If the event is of such magnitude to warrant state assistance, the ISOC will plan and coordinate such response actions. If the event is of a magnitude to involve federal assistance, the ISOC will provide appropriate information to the federal agencies involved.

3. SEF #15 activities will commence with the report (to DISO) of an incident. The level of staffing needed to handle the event will vary depending upon the seriousness of the situation. As the situation develops SEF #15 will initiate information and planning activities and will expand staffing as needed to a partial or full activation of the ISOC.

4. Local, state and, if needed, federal functional counterparts will continuously share operational information.

5. Ensure personnel have appropriate clearances as needed for Secret or Top Secret information and provide a secure location for classified discussions or briefings.

6. Information for dissemination to the public will be coordinated with the designated Lead Public Information Officer (usually the Governor's Press Secretary or COEM Public Information Officer, see annex L). Manipulation of the media and public perception to maximize the psychological impact of violence is a critical element of terrorism – proper, timely public information is critical.

7. SEF #15 will gather, evaluate, and provide essential information necessary for the actions of SEFs participating in the emergency. The local jurisdiction(s), state departments, federal agencies, and others will supply information. Information of common interest and use to the overall emergency and which provides the most complete picture of the overall situation will be displayed and/or made available to all present in the ISOC and any field teams deployed.

   a) Essential elements of information needed by SEF #15 are listed in the Colorado Computer Security Incident Response Team Handbook. Appendix C.

8. SEF #15 will develop Situation Reports (SitReps) that provide a current overall picture of the incident and describe response activities undertaken. SitReps will be disseminated to all jurisdictions, state agencies and others needing the information and will be posted on the ISOC website. SitReps will include the following:

   a) Statistical, narrative and graphical information;
   b) Major response actions taken;
   c) Requests for state assistance by local or other jurisdiction(s)
   d) Priority issues and requirements.

9. SEF #15 will maintain copies of all information to be compiled into a Master Log of the event.

10. As the incident moves from the response phase into the recovery phase, many SEF activities will transition from the ISOC to the impacted agency or agencies.

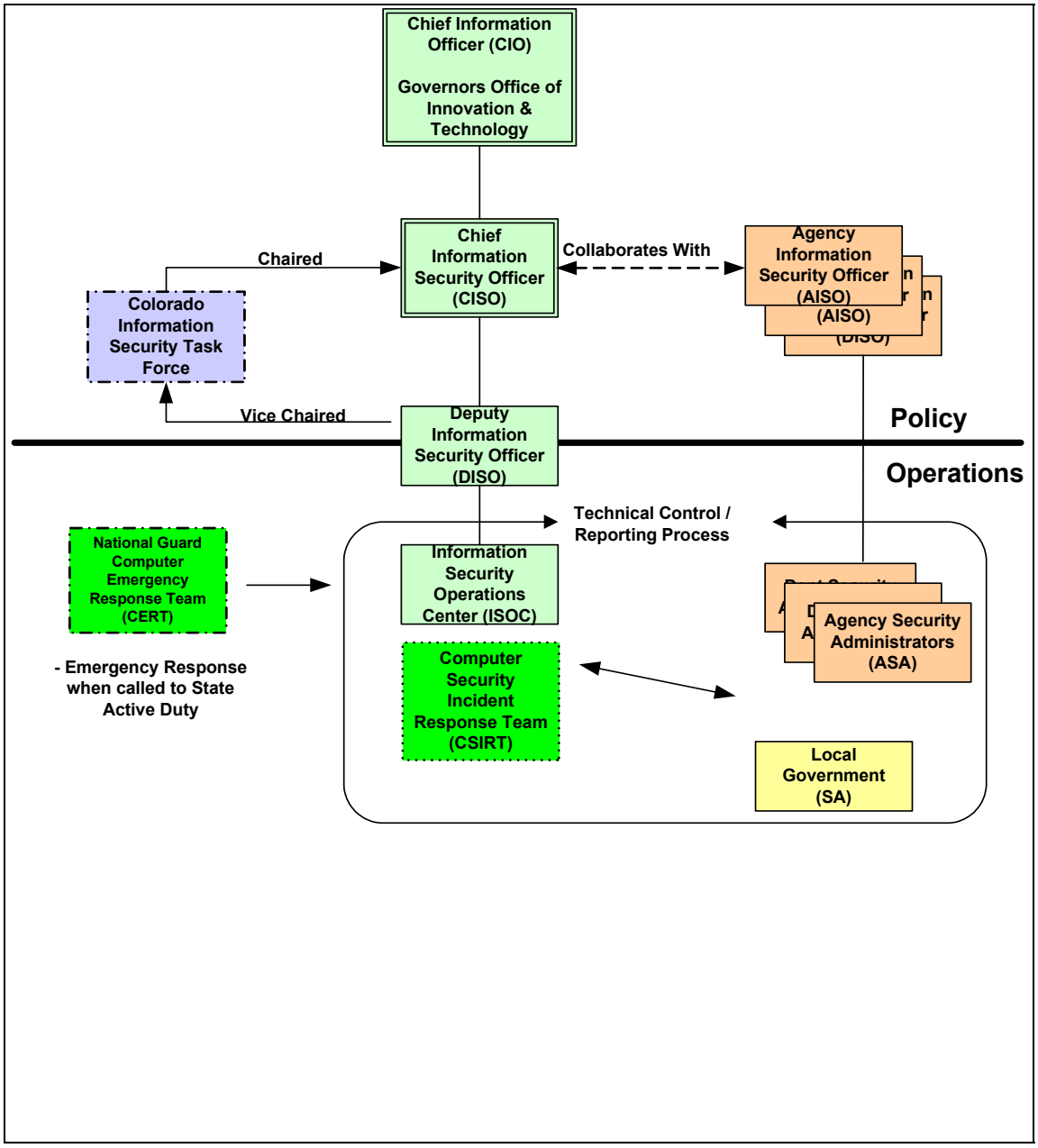
VI. ORGANIZATION and RESPONSIBILITIES

A. Organization

1. SEF #15 activities are conducted, for the most part, in the Information Security Operations Center (ISOC).

2. SEF #15 may consist of one person in the ISOC, (in small events) to an organization consisting of many personnel in the ISOC and departmental Agency Information Security Officers (AISO) and Agency Security Administrators (ASA) (for large events) located in there respective agencies.

3. The following diagram shows the overall information security organizational structure.



B. Responsibilities

1. Department of Personnel Administration/Department of Information Technology Information Security Operations Center (Lead Agency):

a) Coordinate the overall state effort to collect, process, report and disseminate essential elements of information in response to information

security incidents. Establish measures that monitor compliance to best information security best practices.

b) Maintain the state Information Security Operation Center in a state of readiness necessary to properly respond to incidents and to staff SEF #15 during incident situations.

c) Maintain the Colorado State Emergency Operations Plan and provide assistance to other agencies with their related planning responsibilities.

d) To conduct training and exercises to facilitate ISOC activities.

e) To staff the ISOC during activations of any level. If the incident is of a magnitude to require federal assistance, provide a liaison to the FEMA Region VIII ROC or provide a location in the ISOC for a FEMA representative.

2. Support Agencies: ** all impacted agencies**

a) To provide staff necessary to ensure that the organization will be able to respond in incident situations and to participate in training and exercises.

(1) Identify an Agency Information Security Officer (AISO) and provide ISOC with contact information for them. Identify an Agency Security Administrator(s) (ASA) provide ISOC with contact information for them. The ASA must be available for response to the ISOC during incidents.

(2) AISO's and ASA's will participate in training exercises and workshops to maintain a level of proficiency in incident and emergency operations.

b) Maintain an electronic listing of resources. These listings must be available to the AISO, ASA and ISOC during incidents.

VII. APPENDICES

A. Resource Requirements
B. ISOC Position Procedures/Checklists
C. Colorado CIRST Incident Response Handbook - TBP
D. Military Support to Civil Authority

RESOURCE REQUIREMENTS

The following resource requirements are based upon overall needs of SEF #15 to carry out a variety of operational situations. This Appendix is in To Be Published status.

I. Transportation

II. Communications

III. Information Technology resources

ISOC Position Procedures/Checklists

Operations Chief

Responsibilities

1. In consultation with the Deputy Information Security Officer for the State, determine the appropriate level of ISOC staffing and monitor the effectiveness of the organization. Suggest and/or implement changes as necessary.

2. Assume overall management responsibility for the coordination of state incident response efforts. In consultation with the DISO, set priorities for state response and ensure that all actions are accomplished within the priorities established.

3. Keep senior management, CTO, CIO & CISO, informed on all matters regarding the incident and the status of state resources.

4. Keep senior homeland security management and intelligence unit's information on all matters relating to actual or potential terrorism incidents?

Checklist

NOTE: All actions are in consultation with or by direction of DISO.

Activation

- Determine appropriate level of activation and staffing (ISOC and other agencies) needed based on situation information known, including need for external resources.

- Mobilize necessary personnel for additional activation of personnel for the ISOC. Based on escalation procedures.

- Obtain briefing from whatever sources are available.

Start up Actions

- Assign staffs to initiate ISOC check-in procedures, if necessary.

- Provide briefing to all initial staff at ISOC.

- Ensure that the ISOC is properly set up and ready for operations and that necessary computer support is operational.

- Ensure that appropriate security is in place.

- Ensure that telephone and/or radio communications are established with the emergency area.

- Start and maintain an operational log.

- Request additional personnel, as needed, for ISOC staffing and assure that staff has been activated for additional shifts. In Terrorist or National Security activation at least one person per shift should have a security clearance.

Operations Chief

Operational Duties

- Monitor overall situation - both the incident and the ISOC operation.
- Ensure that appropriate information is released to the senior leadership in a timely manner.
- Hold action planning meetings with key staff.
- Provide briefings, as needed, and upon shift changes.
- Ensure that all actions are tracked and completed.
- Keep senior management, and if not available, appropriate Public Safety personnel or Emergency Operations Centers informed on all matters regarding the incident and the status of state resources.

Deactivation

- Authorize deactivation (all or partial) as staff is no longer needed.
- Ensure that all logs and other paperwork are collected from staff departing ISOC.
- Conduct After Action Critique and provide input to After Action Report.

Operations Officer(s)

Responsibilities

Provide assistance to the Operations Chief, as directed by operating computers, taking/making phone calls, tracking incident on logs and status boards, providing information to/from activated SEFs and maintaining communication with the effected agency.

5. Collecting and processing information from the field and ensuring the proper flow of information.

Checklist

Start-up Actions

- Report to Operations Chief for position assignment. Clarify any issues regarding your authority, assignment and the assignments of others.
- Ensure that all equipment in the ISOC is turned on and functioning and that necessary supplies are available.
- Obtain a briefing on the situation and prepare to brief additional ISOC staff as they arrive.
- Start and maintain an operational log.
- Contact SEF representatives and others, as directed by Operations Chief, for response to ISOC. Provide them with a basic overview of the situation to enable them to bring appropriate information.

Operational Duties

- Provide a check-in location for all staff as they arrive at the ISOC; contact and log outside agency representatives and identify their work location; ensure that outside agency representatives understand their assigned function and give situation briefing upon contact so that they may begin operation.
- Monitor and prioritize all information as it comes to the Operations Desk (either by e-mail, phone, wireless, or paper) and ensure that Operations Chief and other ISOC staff receive necessary information.
- Act as point-of-contact for telephone calls from impacted agencies.
- Respond to requests from other agencies and from the field.
- Maintain a list of all personnel in the ISOC and their working location/phone extension.

Operations Officer(s)

- Ensure that there is appropriate staff on-call for additional shifts.
- Ensure that all SEOC staff are fed and that breaks are taken to avoid over-fatigue.

Deactivation

- Release staff (ISOC and other agencies) as Operations Chief directs.
- Get a forwarding phone number from each ISOC staff person before they leave.
- Collect all logs and paperwork for permanent record of event.
- Archive all computerized data (e-mail, EIS, and any other) for use in permanent event record.
- Attend and provide input to the After Action Critique and After Action Report.

Agency Security Administrators (ASA)

NOTE: This procedure is generic to all outside agency representatives responding to ISOC activation. It is designed to be supplemented by each agency's own checklist or procedures.

Responsibilities

1. An agency representative may be the Lead of a State Emergency Function or a support agency.

2. They must be knowledgeable of the functions, and capabilities of their agency in the area of information and network security.

Checklist

Start-up Actions

- Make communications with ISOC Operations Officer determine the location of your work area. and all necessary contact information.

- Obtain current situation briefing from the person you are relieving or from the Operations Officer.

- Clarify any issues regarding your authority, assignment and the assignments of others.

- Check workstation for supplies; floor plan, phone listing, ISOC information, notepad, pencils, etc.

- Start and maintain an operational log.

- Establish contact with your agency and, if necessary, clarify your decision-making authority.

Operational Duties

- Facilitate and track requests for assistance or information that your agency can provide.

- Keep up-to-date with the status of resources and activity associated with your agency.

- Provide appropriate situation information to the Operations Chief through the Operations Officer by any communications means and by entering it into the operations log.

- Provide your agency appropriate situation information on ISOC priorities and actions.

- Attend Action Planning Meetings if requested.

Deactivation

Agency Representatives

- Turn in all logs and other paperwork for inclusion in the permanent record.

- Check out with ISOC Operations officer and leave a forwarding phone number.

- Attend and provide input to the After Action Critique and After Action Report.

Appendix D to Annex O
Military Support to Civil Authority

I. PURPOSE

This annex provides guidance for the use of Military Support to Civil Authority (MSCA) in Colorado. It applies to Colorado Army and Air National Guard, Civil Air Patrol, and active and reserve military units in the state.

II. SITUATION

A. The Governor is the Commander in Chief of the Colorado National Guard and may authorize activation of forces to save lives and property.
B. The National Guard has armories located throughout the state with the Headquarters located in the Centennial area.
C. Civil Air Patrol is a division of Colorado State Government (Department of Military & Veterans Affairs) with the Wing Commander as Division Director.
D. Military reserve forces are stationed in Colorado.
E. There are six U.S Army and Air Force installations located in Colorado.

III. ASSUMPTIONS

A. Local authorities will request military assistance only when local resources and mutual aid assistance are inadequate or have been exhausted.
B. Members of active and reserve forces stationed in Colorado may be victims of the disaster and hence not available for response.
C. National Guard assistance is short-term and will not be used in place of private resources.
D. Federal activations may limit the availability of personnel and equipment within the state.

IV. CONCEPT OF OPERATION

A. National Guard may provide assistance when activated in only two ways; 1) by order of the Governor or his designated representative and 2) a local commander may respond on his own authority in times of live saving emergencies.
B. The military chain of command and unit integrity will remain in effect and local authorities will not supplant military authority over military personnel.
C. An Emergency Response Coordinator from the National Guard will be present in the state EOC if requested by Colorado OEM.
D. The National Guard will have a representative in the Incident Command Center.
E. Requests for National Guard assistance will be made by calling the Colorado OEM on the state emergency line at 303-279-8855.
F. Requests for Civil Air Patrol will be made by the local jurisdiction calling the Air Force Rescue Coordination Center (AFRCC) 800-851-3051 for search and rescue missions or Air Force National Security Emergency Preparedness (AFNSEP) 800-366-0051 for coordination and mission assignment of other types of missions.
G. Requests for active or reserve military forces will be made through Colorado OEM to FEMA Region VIII to NORTHCOM.

V. RESPONSIBILITIES

A. Colorado National Guard
    1. When activated by the Governor, provide manpower and equipment to assist in emergency situations.
    2. Maintain detailed financial records for reimbursement purpose.

B. Colorado OEM

1. Verify/validate all requests for National Guard Assistance. Make request/recommendation for activation to Governor (delegate).
2. Coordinate approved assistance with the National Guard.
3. Verify/validate all requests for active and reserve military assistance. Coordinate request for activation through FEMA.
4. Provide payment (when authorized) from the State Disaster Fund.

C. Local Jurisdictions

1. Requests for National Guard will only be when all other sources of assistance, including private contractors, have been exhausted.
2. Provide detailed information on the incident, actions already taken, and what is needed.