Cyber Liaison Officer (CLO) Course – Cyber Crimes

**When:** Thursday March 19, 2019; 8:00AM-5:00PM

**Where:** San Mateo Police Dept.

200 Franklin Parkway

San Mateo, CA 94403

**Presenter:** Northern California Regional Intelligence Center (NCRIC)

**Course Description:** Today’s law enforcement must be equipped to identify and defend against the growing threat of cyber crime. First responders encountering cyber crimes are uniquely positioned to document, collect, and report details that can impact subsequent investigation and court testimony. The Cyber Liaison Officer (CLO) Course is a 1-day class that provides law enforcement officers with strategies to build strong cases involving phones, computers, networks, servers, or IP addresses. Participants will learn common cyber criminal tactics including business email compromise (BEC) and ransomware, how to analyze an email header, how to tie an IP to a physical address and person, and how to recognize a network intrusion. Students will go through the process of responding to a call with a potential cyber nexus, what questions to ask when interviewing victims/witnesses, and identifying evidence to continue an investigation.

A Cyber Liaison Officer is any Active peace officer, firefighter, state investigator, federal agent, military investigative personnel, or anyone working closely within the public safety / homeland security community, who has been properly certified by the appropriate Regional Threat Assessment Center (RTAC) / Regional Intelligence Center (RIC). The mission of a Cyber Liaison Officer is to serve as a conduit of information between members of the public safety community, public/private sector, citizenry and the US Government, in the fight against terrorism.

**Course Objectives:**

- Identify and document the necessary information about cyber crime
- Identify and apply basic cyber security concepts
- Identify appropriate stakeholders/resources to contact when a cyber crime occurs

- Have a clear understanding of the laws about search and seizure of electronic evidence

- Determine how to handle evidence collected from a cyber crime

**Target Audience / Discipline:** This instruction is designed for Active Peace Officers, Firefighters, State Investigators, Federal Agents, Military Investigative personnel, or other government employees working within the public safety / homeland security community. Attendees must be currently employed by a government agency operating in the NCRIC's Area of Responsibility (AOR) - see below.

**Cost:** FREE

**Attendance:** Limited to employees within the NCRIC's Area of Responsibility (AOR), which consists of Alameda, Contra Costa, Del Norte, Humboldt, Lake, Marin, Mendocino, Monterey, Napa, San Francisco, Santa Clara, Santa Cruz, San Benito, San Mateo, and Sonoma counties.

**Registration:** Registration must be completed on-line at [www.ncric.ca.gov](http://www.ncric.ca.gov) in the Members Only section (if you are not a member, click on the link to join). Click on the "Registration" Tab.

All attendees are automatically placed on a waiting list and will be notified by email of their acceptance and registration in the course. No "walk up" registrations accepted.

**This course is POST Certified.**

Questions? Call or email.

Alison Yakabe
Lead Cyber Intelligence Analyst
ayakabe@ncric.ca.gov
415-470-3628