CHAPTER 12

COMPUTER CRIMES INVESTIGATION UNIT

REVISED FEBRUARY 2024

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 12

COMPUTER CRIMES INVESTIGATION UNIT

1. GENERAL.

a. The constantly evolving world of computer technology provides an enormous variety of hardware, software, and information that can be utilized by both average and sophisticated criminals to facilitate criminal activities. Current and past cases, at the state and national levels indicate that high-technology theft and computer-related crimes are commonplace. With the expansion of the Internet into all areas of personal and business life, computers and other electronic media are commonly used to commit criminal acts (e.g., hacking, identity theft, malicious code). Additionally, evidence of criminal activity not traditionally thought of as a computer crime can be found on almost any form of electronic media (e.g., portable storage devices, gaming consoles, vehicle computer systems, cell phones, printers, cameras).

b. Government Code Section 14613.7(a) requires state agencies to report to the Department all crimes on state-owned or state-leased property where state employees are discharging their duties. This includes the reporting of crimes involving state computer resources.

c. The Computer Crimes Investigation Unit (CCIU) is assigned to Information Management Division. This specialized unit investigates computer-related crimes and threats against California's information technology infrastructure.

d. The primary responsibility of CCIU is the investigation of any criminal activity in violation of Section 502 of the California Penal Code (PC) (refer to Annex A of this chapter), involving state-owned or state-leased computers, computer networks, computer systems, or data stored on electronic media devices. The CCIU also provides computer forensic services to the Department's field commands and other investigative units.

e. The content of this chapter establishes policy that governs the overall process in which forensic examinations are conducted involving items of electronic media.

2. POLICY.

a. The CCIU is primarily responsible for conducting criminal investigations involving state computer assets associated with violations of Section 502 PC. Additionally, CCIU shall be the primary resource for the forensic examination of all

electronic media associated with criminal and administrative investigations being conducted by departmental personnel.

b. The Department will examine items of electronic media used or allegedly used in the commission of crimes or that otherwise contain data to support an investigation being conducted by departmental personnel. The examinations being conducted shall be done for the purpose of determining if the item of electronic media contains information (data) of evidentiary value and to legally preserve the information (data) as evidence.

c. Information Management Division is the Office of Primary Interest for all forensic examinations of electronic media being conducted by departmental personnel.

d. Field division commanders may assign field division personnel to conduct forensic examinations of electronic media associated with departmental investigations. If such assignments are made, however, the field division commander shall be responsible for ensuring the assigned personnel have the necessary training, experience, and equipment to ensure the integrity of such examinations due to constantly evolving computer hardware and software technology and computer forensics techniques.

3. TRAINING.

a. Officers assigned to conduct forensic examinations of electronic media shall be required to attend sufficient training to establish their expertise in the field of computer crimes investigation and computer forensics.

b. The required training courses include, but are not limited to, those designated by the Commission on Peace Officer Standards and Training; Robert Presley Institute of Criminal Investigation, in the specialty of Computer Crimes Investigation; the California Department of Justice, Advanced Training Center; and the United States Secret Service, National Computer Forensics Institute.

4. PROCEDURES FOR REQUESTING ELECTRONIC MEDIA FORENSIC.

a. Forensic Examination of Electronic Media. All forensic examinations of electronic media for the purpose of obtaining criminal evidence, intelligence, data, or the existence of or configuration of specific hardware or software, should normally be done with a search warrant specifically authorizing the search and seizure of the particular media.

b. Preplanned Incident Request. If a member of the Department intends to seize a computer system, its contents, other items of electronic media, or is intending to serve a search warrant where the possibility of seizing such items exists, a CCIU investigator should be contacted for assistance. Assistance from the CCIU can include planning, coordination, and seizure of the items of electronic media in addition to the acquisition and preservation of electronic evidence. If the requests for assistance are beyond that of advice, for example, about processes or search warrants, such requests should be made by an appropriate departmental manager to the CCIU manager or supervisor. The CCIU manager or supervisor will determine if additional approvals are needed to provide the requested assistance.

c. Unplanned Incident Request. After business hours requests for CCIU assistance can be made to the CCIU manager or supervisor through the Emergency Notification Tactical Alert Center.

d. Allied Agency Request for Assistance. All requests for assistance from allied agencies may be directed to the CCIU manager or supervisor for evaluation and recommendation. The CCIU manager or supervisor shall determine if the Department will provide assistance to allied agencies or if the request requires additional approvals. These decisions will be made while considering the following:

(1) The Department's mission and objectives.

(2) Scope of expertise.

(3) Available resources.

(4) Case information/scenario.

(5) Scope of investigation.

e. Seizure. There should normally be no examination, powering up, "booting" or other inspection of the computer, media storage devices, or related peripherals, except by personnel specifically trained in the forensic examination of computer systems and data. Operation of the suspect computer by untrained personnel without the proper software in an uncontrolled environment may compromise data and any chain-of-evidence. Further, any evidence on the computer or storage media may be rendered unusable in criminal, civil, or administrative proceedings.

f. Taking Possession of Seized Electronic Media. In most cases, the CCIU will take possession of seized items of electronic media and conduct a forensic analysis. The analysis will take place in a secure environment, under forensically and controlled conditions, using methodology and techniques in use by the computer forensic community.

g. Storage of Evidence Associated with Forensic Examinations. Normally, when the services of the CCIU are requested to conduct forensic examinations of electronic media by other departmental or allied agency entities; the original evidence, along with evidentiary copies of the associated electronic media, will be returned to the entity requesting assistance for long term storage and disposition upon completion of the examination process. In some cases, depending on the volume of storage media required for evidentiary copies, the entity requesting assistance may be required to provide the necessary storage media as determined by the CCIU.

ANNEX A

CALIFORNIA PENAL CODE SECTIONS 502 (b) AND (c)

502.(b). For the purposes of this section, the following terms are defined by the following:

(1) Access. To gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

(2) Computer Network. Any system that provides communications between one or more computer systems and input/output devices, including, but not limited to, display terminals, remote systems, mobile devices, and printers connected by telecommunication facilities.

(3) Computer Program or Software. A set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(4) Computer Services. Includes, but is not limited to, computer time, data processing, or storage functions, internet services, electronic mail services, electronic message services, or other uses of a computer, computer system, or computer network.

(5) Computer System. A device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control. A “computer system” includes, without limitation, any such device or system that is located within, connected to, or otherwise integrated with, any motor vehicle as defined in Section 415 of the Vehicle Code.

(6) Government Computer System. Any computer system, or part thereof, that is owned, operated, or used by any federal, state, or local governmental entity.

(7) Public Safety Infrastructure Computer System. Any computer system, or part thereof, that is necessary for the health and safety of the public including computer systems owned, operated, or used by drinking water and wastewater treatment facilities, hospitals, emergency service providers, telecommunication companies, and gas and electric utility companies.

(8) Data. A representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or stored in the memory of the computer or in transit or presented on a display device.

(9) Supporting Documentation. Includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.

(10) Injury. Any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or the denial of access to legitimate users of a computer system, network, or program.

(11) Victim Expenditure. Any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.

(12) Computer Contaminant. Any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

(13) Internet Domain Name. A globally unique, hierarchical reference to an Internet host or service, assigned through centralized Internet naming authorities, comprising a series of character strings separated by periods, with the rightmost character string specifying the top of the hierarchy. comprising a series of character strings separated by periods, with the rightmost character string specifying the top of the hierarchy.

(14) E-mail. An electronic message or computer file that is transmitted between two or more telecommunications devices, computers, computer networks, regardless of whether the network is a local, regional, or global network, or electronic devices capable of receiving electronic messages, regardless of whether the message is

converted to hard copy format after receipt, viewed upon transmission, or stored for later.

(15) Profile. Includes A) a configuration of user data retrieved by a computer so that the user may access programs or services and have the desired functionality on that computer, and B) an Internet website user's personal page or section of a page that is made up of data, in text or graphical form, that displays significant, unique, or identifying information, including, but not limited to, listing acquaintances, interests, associations, activities, or personal statements.

502.(c). Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to, A) devise or execute any scheme or artifice to defraud, deceive, or extort; or B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys, any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

(10) Knowingly and without permission disrupts or causes the disruption of government computer services or denies or causes the denial of government computer services to an authorized user of a government computer, computer system, or computer network.

(11) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a public safety infrastructure computer system computer, computer system, or computer network.

(12) Knowingly and without permission disrupts or causes the disruption of public safety infrastructure computer system computer services or denies or causes the denial of computer services to an authorized user of a public safety infrastructure computer system computer, computer system, or computer network.