CHAPTER 5

MALWARE PREVENTION AND PROTECTION

REVISED NOVEMBER 2025

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 5

MALWARE PREVENTION AND PROTECTION

1. GENERAL.

a. Purpose and Scope. This document identifies the risk malicious software poses to the Department's Information Technology (IT) infrastructure and defines the measures the Department must take to mitigate the risk of malware in the environment.

b. Malware Definition. Malware is any software intentionally designed to cause damage to a computing device (e.g., desktops, laptops, tablets, and telephones), application, service, database, or computer network. Malware causes damage after it is implanted or introduced into a target's computing device and can take the form of executable code, scripts, active content, and other software. The code is described as worms, Trojan horses, ransomware, spyware, adware, and scareware, among other terms. Malware performs malicious actions that act against the interest of the computing device owner. Malware does not include software that causes unintentional harm due to a deficiency, which is typically a software bug.

(1) Common forms of malware include, but are not limited to, the following:

(a) Viruses. A computer virus is a software program that's usually hidden within another seemingly innocuous program that can produce copies of itself. The copies are inserted into other programs or files and then typically perform a harmful action, such as destroying data.

(b) Ransomware. A type of malicious software, ransomware threatens to publish a victim's data, or perpetually block access to it, unless a ransom is paid. While some simple ransomware may lock the system in a way that can be reversed, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files, making them inaccessible, and demands a ransom to decrypt them.

(c) Spyware. Operating in the background, spyware is a type of malicious software that aims to gather information about a person or organization without their knowledge. Spyware may send such information to another entity without the consumer's consent or assert control over a device without the consumer's knowledge. Spyware is primarily classified into four types: adware, system monitors, tracking cookies, and Trojans. Other types of spyware include digital rights management capabilities that collect sensitive data and exfiltrate it to a bad actor.

1 Adware. Numerous software vendors have turned to making money from computer advertisements instead of selling software licenses. Many of these software titles promise more than they deliver and frequently have malicious components.

(d) Advanced Persistent Threat. An Advanced Persistent Threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity. An APT usually targets private organizations, states, or both for business or political motives. The APT processes require a high degree of stealth over a long period of time. The "advanced" process includes sophisticated techniques using malware to exploit vulnerabilities in systems. The "persistent" process is an external command and control system continuously monitoring and extracting data from a specific target. The "threat" process indicates human involvement in orchestrating the attack.

(2) Department Risk from Malware. The Department faces many risks and liabilities regarding information security, including but not limited to, the following:

(a) Availability. When computing devices become infected or compromised, they must be removed from service and analyzed for security reporting until they can be returned to the default configuration. One infected computing device can cause a lateral infection across the infrastructure to many computing devices and servers. If faced with a pandemic situation, the Department may be without its computing devices. In a worst-case scenario, the damage is inflicted in exponential scales.

(b) Confidentiality. Some malicious software is specifically designed for intelligence-gathering and is frequently designed to discover sensitive information on a victim's computing device, such as usernames, passwords, and personally identifying information, or to completely liquidate data. Once infected, computing devices may begin reporting the activities of its user to the person in charge of the malicious software. If data is copied and/or removed from the victim's computing device, the Department could experience a loss in public trust.

(c) Integrity. When malicious software is found on a computing device, the computing device's integrity is compromised and is no longer intact. If the Department has a cybersecurity incident that goes public, it could undermine public confidence in the information security of the CHP.

(3) Social Engineering. Modern computer security has prevented most mundane malware attacks. Bad actors use social engineering—or the act of conversing with an unwilling participant to encourage an unsuspecting person

to run malicious software—to gather information not readily available as public knowledge. Common forms of social engineering include phishing, spear phishing, and APTs.

(a) Phishing. Bad actors send specific and targeted e-mails to users in hopes of tricking them into providing additional information; this is known as a spam attack. When sent via text message, it is called smishing, and when sent by voice call, it is called vishing.

(b) Spear Phishing. Spear phishing is much like phishing except the messages are specifically crafted for the individual targeted. As the attacker gains information on their target, they can craft specific attacks. For example, an attacker can use Facebook information to identify potential friends of a target, then pose as a friend and use that trust to send a malicious file to the target.

(c) Advanced Persistent Threat. An APT is a human-orchestrated attack where one or more people organize and collect data on a target. Information is pooled together and used to coordinate targeted cyberattacks within the organization.

c. Responsibilities.

(1) Department Responsibilities. The Department is responsible for the health and maintenance of its computing devices in accordance with Statewide Administrative Manual, Section 5300, Information Technology – Office of Information Security. Failure to maintain a safe and secure computing environment will damage the credibility and reputation of the Department's IT programs.

(2) Technology Infrastructure Section Responsibility. The Department's Technology Infrastructure Section (TIS) is responsible for providing a centralized endpoint protection solution. An endpoint protection solution shall be deployed to all workstations and servers supported by TIS and will be kept up-to-date and maintained.

(3) User Responsibilities. It is the responsibility of all users of departmental computing devices to maintain and follow good security practices to avoid issues involving malware. Computing devices that do not have an updated endpoint protection solution shall not access the Department's network.

(a) Departmental computing devices must regularly be connected to the Department's network to receive software updates.

(b) Employees shall not connect unapproved hardware to the Department's network.

(c) Employees shall not run unapproved software on departmental computing devices.

(d) Employees shall not open unexpected or unidentified files on departmental computing devices.

(e) Employees shall report any abnormal behaviors of computing devices to the Department's IT Support Unit at (916) 843-3899 or ITSupport@chp.ca.gov.