

Memorandum of Understanding

Between

California Governor's Office of Emergency Services

and

County of Humboldt

Information Technology Division

PREAMBLE

This Memorandum of Understanding (MOU) sets forth the terms and conditions between the Governor's Office of Emergency Services (Cal OES), on behalf of the California Cyber Security Integration Center (Cal-CSIC), and County of Humboldt (Partner) (collectively "party" or "parties") regarding participation in information sharing activities of Cal-CSIC.

I. BACKGROUND

- A. The Cal-CSIC was established, under California Governor's Executive Order B-34-15, codified by Government Code section 8586.5, to reduce the likelihood and severity of cyber incidents that may significantly compromise the security and resilience of California's economy, its critical infrastructure, or public and private sector information and communications technologies. Government Code section 8586.5 provides that Cal-CSIC shall coordinate information sharing with local, state and federal agencies, tribal governments, utilities and other service providers, academic institutions, and non-governmental organizations to reduce the likelihood and severity of cyber-attacks.
- B. The ability to share threat and vulnerability information provides the Cal-CSIC insight into historical threat trends and best mitigation practices. This is essential to understanding threat actors and vectors of attack, allowing the Cal-CSIC to effectively provide indications and warning and aid in preventing the occurrence of cyber incidents.

II. **PURPOSE**

- A. This MOU will formalize the information sharing partnership between Cal OES on behalf of the Cal-CSIC and Partner.
- B. This MOU is an agreement between Cal OES, on behalf of the Cal-CSIC, and Partner.

III. **RESPONSIBILITIES:**

- A. Protect California and Partner interests, information systems, and data;
- B. Establish authorities, roles, and responsibilities regarding the sharing of cyber threat and vulnerability information;
- C. Adhere to the laws, policies, processes, and procedures regarding how information will be shared, transmitted, stored, used, maintained, and destroyed;
- D. Identify and provide information sources to be used within the Cal-CSIC and classify source data;
- E. Define access controls and determine the "Need-to-Know" of other Cal-CSIC partners; and,
- F. Resolve risks and liabilities associated with the activities outlined in this MOU.
- G. The Parties agree:
 - i. The Cal-CSIC and Partner shall identify information sources and determine the most secure, appropriate, and effective means of sharing that information;
 - ii. Partner shall inventory and make information sources available to the Cal-CSIC for collection and analysis;
 - iii. With the approval of the Partner Information Security Officer or equivalent role, Partner personnel shall follow the Cal-CSIC-recommended procedures for generating event data for transmittal to Cal-CSIC;

- iv. The Cal-CSIC shall utilize highest data security controls to protect Partner information against unauthorized access or acquisitions;
- v. The Cal-CSIC shall store and use information in accordance with all laws, policies, standards, and guidelines, applicable to the information, and will comply with lawful restrictions Partner places on the sharing or use of shared indicators or defensive measures as set forth by Partner in this MOU;
- vi. Information derived from Partner sources containing target or vulnerability information will not be shared outside of Cal-CSIC and Partner communications;
- vii. Cal-CSIC and partner agree that as a stipulation of this MOU, that both Cal-CSIC and partner shall not use the shared data between Cal-CSIC and partner for commercial use or for financial gain.
- viii. Cal-CSIC and partner agree that as a stipulation of this MOU, that both Cal-CSIC and partner shall not copy, modify, distribute, or display shared data between Cal-CSIC and partner for commercial use or financial gain.
- ix. Implicit or unaffiliated threat and vulnerability information derived from Partner sources may be shared with other Cal-CSIC partners if information provides benefit to the overall security of California residents, economy, and government;
- x. The Cal-CSIC will share threat indicators with law enforcement officials to prevent, investigate, or prosecute offenses including but not limited to: (1) an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or use of a weapon of mass destruction; or (2) crimes involving fraud and identity theft, espionage and censorship, or trade secrets;
- xi. The Cal-CSIC shall remove or anonymize personal information, or information that identifies a specific person not directly related to a cybersecurity threat, prior to sharing an indicator unless compelled to release such information by law or at the direction of law enforcement; and
- xii. The Cal-CSIC shall share threat indicators and defensive measures with Partner solely for the purposes of:

1. Protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability;
2. Identifying a cybersecurity threat, including the source, or a security vulnerability;
3. Identifying the use of an information system by a foreign adversary or terrorist;
4. Responding to, or otherwise preventing or mitigating, a serious threat to a minor or an imminent threat of death, serious bodily harm, or serious economic harm, including but not limited to a terrorist act or a use of a weapon of mass destruction; or
5. Preventing, investigating, disrupting, or prosecuting an offense arising out of an imminent threat of death, serious bodily harm, or serious economic harm, as well as offenses relating to fraud and identity theft, espionage and censorship, or trade secrets.

xiii. Partner will grant Cal-CSIC access to the following information:

1. Network traffic metadata generated by on premise security appliances
2. Partner Relevant vulnerability assessment and security audit reports.
3. Partner shall provide human-readable threat notifications and reports.
4. Partner shall provide the Cal-CSIC with the names, email addresses, and telephone numbers of primary consumers of threat intelligence.

IV. **PRIVACY AND LIBERTIES**

- A. Partner agrees to abide by the Traffic Light Protocol (TLP) label on all of the Cal-CSIC threat reports, when sharing. Explicit permission from the Cal-CSIC must be obtained if Partner intends to share beyond what is specified in the TLP label. TLP labels are described

below:

- i. TLP: RED – Limited to those with direct access to said information, or have been specifically given the information.
- ii. TLP: AMBER – may be shared with members of their own organization who need to know, and only as widely as necessary to act on that information.
- iii. TLP: GREEN – may be shared with peers and partner organizations within their sector or community, but not via publicly accessible channels.
- iv. TLP: WHITE – may be distributed freely, without restriction.

B. Disclosure of Information

- i. As a state agency, Cal OES is required to comply with California Public Records Act ("PRA"), Government Code sections 6250 et seq. Records of Cal OES are thus controlled by the provisions of the PRA. Unless the records are exempt under the PRA, Cal OES must make them available for public inspection.
- ii. Confidential information—information that may be exempt from disclosure to the public or other unauthorized persons under state and/or federal statutes—shall be clearly marked. Exchange of such information pursuant to this MOU is not a public disclosure under the PRA. When confidential information is exchanged, it shall be used and accessed only for the limited purposes of carrying out activities pursuant to this MOU.
- iii. Partner agrees that if they receive a request under California Public Records Act, Government Code §§ 6250, et seq., for records containing information provided by Cal OES and/or Cal-CSIC under this MOU, Partner shall notify Cal OES, and provide a reasonable time for Cal OES to review the records

responsive to the California Public Records Act request prior to Partner's disclosure of any information.

V. REPORTING

- A. The Cal-CSIC Governance Stewards are responsible for determining the quality and level of partner support to the Cal-CSIC activities and will evaluate whether information requirements are met by sources outlined in this MOU.
- B. The Cal-CSIC Cyber Analyst Team will track intelligence derived from partner sources and provide an overview of validation and sufficiency to the Governance Stewards on an annual basis. This information may be used to drive better information sharing opportunities and agreements.

VI. EFFECTIVE DATE, DURATION AND MISCELLANEOUS PROVISIONS

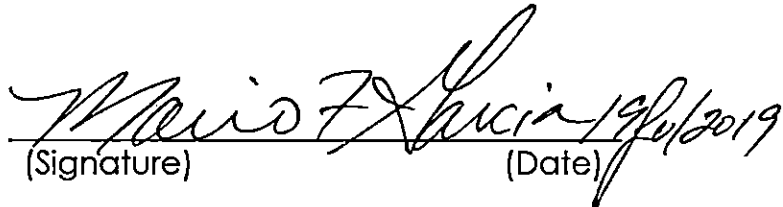
- A. This MOU is effective upon signature of the Parties.
- B. This MOU may be dissolved at any time, in writing, by the Parties.
- C. This MOU may be modified at any time, in writing, by mutual consent of the Parties in order to accommodate changing circumstances.
- D. All modifications to this MOU must be recorded in writing and signed by the Parties.
- E. This MOU does not entitle the Parties to any rights they would not otherwise have under the law. This MOU does not create any obligations for the Parties other than as stated herein. This MOU should not be construed to create or confer on a third party any right or benefit, substantive or procedural, enforceable at law or otherwise, against the Parties.
- F. The MOU is subject, as applicable, to the laws of the State of California.
- G. This MOU is not a commitment of funds.

Contact Information

Governor's Office of Emergency Services
Mario F. Garcia
Acting Commander, California Cybersecurity Integration Center
3650 Schriever Ave
(916) 636-2928
mario.garcia@caloes.ca.gov

County of Humboldt
Jim Storm
IT Division Director
839 4th Street, Eureka, CA 95501
707.268.3674
jstorm@co.humboldt.ca.us

(Signature)
(Date)
Jim Storm
IT Division Director
County of Humboldt


(Signature) (Date) 19/01/2019
Mario F. Garcia
Deputy Commander
California Cybersecurity Integration
Center
Governor's Office of Emergency
Services