GAVIN NEWSOM
GOVERNOR

NANCY WARD
DIRECTOR

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

June 27, 2024

The Honorable Melissa Hurtado
California State Senator
Senate District #16
1021 O Street, Suite 8630
Sacramento, CA 95814

The Honorable Freddie Rodriguez
Chair, Assembly Committee on
Emergency Management
1020 N Street, Room 360B
Sacramento, CA 95814

The Honorable Bill Dodd
Chair, Senate Committee on
Governmental Organization
1020 N Street, Room 584
Sacramento, CA 95814

Mr. Gabriel Petek, Legislative Analyst
Legislative Analyst's Office
925 L Street, Suite 1000
Sacramento, CA 95814

Subject: Report to California Legislature Regarding Cybersecurity Outreach Strategy to Food and Agriculture, Water & Wastewater Critical Infrastructure Sectors (SB-892)

Dear Senators, Assemblymember and Legislative Analyst:

Pursuant to Government Code Section 8592.50, the California Office of Emergency Services (Cal OES) is required to direct the California Cybersecurity Integration Center (Cal-CSIC) to prepare, and Cal OES to submit to the Legislature a strategic, multiyear outreach plan to assist the food and agriculture (FA) sector and the water and wastewater (W&WW) sector in their efforts to improve cybersecurity and an evaluation of options for providing entities in the FA sector or the W&WW sector with grants or alternative forms of funding to improve cybersecurity preparedness.

Should you have any questions, please contact Deputy Director of Legislative and Governmental Affairs, Bridget Kolakosky at (916) 364-4635 or bridget.kolakosky@caloes.ca.gov.

Sincerely,

Nancy Ward

NANCY WARD
Director
cc: Ann Patterson, Cabinet Secretary, Office of the Governor

EMERGENCY MANAGEMENT EMAP Accredited ACCREDITATION PROGRAM
3650 SCHRIEVER AVENUE, MATHER, CA 95655
(916) 845-8506 TELEPHONE (916) 845-8511 FAX
www.CalOES.ca.gov

REPORT TO CALIFORNIA LEGISLATURE

REGARDING MULTIYEAR OUTREACH PLAN REQUIRED BY SENATE BILL 892

CAL-CSIC OUTREACH PLAN TO FOOD AND AGRICULTURE, WATER AND WASTEWATER CRITICAL INFRASTRUCTURE SECTORS AND AN EVALUATION OF GRANTS OR ALTERNATIVE FORMS OF FUNDING

January 1, 2024

Contents

1 Executive Summary 1
2 Need for Greater Cybersecurity Outreach 2
2.1 Scale of California's FA Sector 2
2.2 FA Cybersecurity Threat Landscape 2
2.3 Scale of California's W&WW Sector 2
2.4 W&WW Cybersecurity Threat Landscape 3
3 Goal Of the Outreach Plan 4
3.1 Strategic, Multiyear Outreach Plan 4
3.2 Descriptions of Phase By Year 5
4 Methods For Coordinating with Partners 10
5 Estimate Of Funding 10
6 Potential Funding Sources for Outreach Plan 11
7 Plan To Evaluate Success of Outreach Plan 11
8 Evaluation Of Grants or Alternative Forms of Funding to Improve Cybersecurity Preparedness 13
8.1 Summary Of Evaluation Performed by Cal-CSIC 13
8.2 Listing Of Funding Sources (Grants or Alternatives) for Improved Cybersecurity Preparedness 13
8.3 Potential Voluntary Actions 16
9 Conclusion 17

1 Executive Summary

The following report is submitted pursuant to Senate Bill 892 (Hurtado Statutes of 2022), which requires the Office of Emergency Services (Cal OES) to task the California Cybersecurity Integration Center (Cal-CSIC) to prepare, and Cal OES to submit to the Legislature, a multiyear strategic outreach initiative. The outreach initiative is aimed at bolstering cybersecurity within the sectors of food and agriculture (FA) as well as water and wastewater (W&WW). Moreover, this report will evaluate options for providing entities in the FA or W&WW sector with grants or alternative forms of funding to improve cybersecurity preparedness.

Cybersecurity in the critical infrastructure sectors is inherently complex due to a myriad of factors. The Department of Homeland Security (DHS) provides a tool for understanding this complexity called the Infrastructure Data Taxonomy, providing a breakdown of each sector to its individual parts through several levels of categorization. This taxonomy is organized into four levels: sectors, subsectors, segments, and subsegments. Each level is increasingly narrow and specific. The California FA sector has 8 subsectors, 42 segments, and 105 sub-segments. If all data points from all combinations are combined from FA and W&WW, there are approximately 507 distinctly complex technology areas to analyze, prioritize, and scope.

The FA and W&WW sectors are vast, and the FA sector alone has a major role in the California economy and in feeding the world. The interconnectedness of these critical systems, which amplifies the impact of cyber attacks must also be considered. Addressing these complexities demands a comprehensive outreach approach that embraces collaboration, innovation, and resilience-building efforts to mitigate cyber threats effectively.

This report will give a glimpse into the intricacies of both the FA and W&WW sectors. It should be noted that additional analysis of these two sectors alone will require assistance from additional partner organizations and non-governmental organizations (NGO) with subject matter expertise in the aforementioned sectors. The magnitude of this analysis is beyond the understanding of the Cal-CSIC and the State Threat Assessment Center (STAC). Prior to the requirement of this report, the Cal-CSIC conducted limited outreach. However, the Cal-CSIC understands the value in additional outreach as it will improve community security as well as the Cal-CSIC and STAC's threat awareness and ability to counter cybersecurity threats.

Throughout this assessment, the Cal-CSIC and its partners will describe a flexible, but achievable, multi-year outreach, as well as an evaluation of potential success. Finally, the report will enumerate associated costs and available funding opportunities for overall improved cybersecurity preparedness.

2 Need for Greater Cybersecurity Outreach

For purposes of this report, outreach will be defined as "the extending of services or assistance beyond current or usual limits." In an effort to apply this definition to the FA and W&WW sectors, service or assistance will include cybersecurity education, awareness, and improved access to resources to improve cybersecurity. The analysis of these sectors requires the time and resources necessary to complete an effective "Prioritization and Scoping Phase."

2.1 Scale of California's FA Sector

An understanding of California's FA and W&WW sectors were vital, prior to the development of the strategic, multi-year outreach plan. According to the 2021-2022 Agricultural Statistics Review produced by the CDFA[1], California's FA sector earned $51.1 billion in cash receipts for the 2021 crop year and exports totaled $22.5 billion. Additionally, California's agricultural economy supports more than 1.2 million jobs.

2.2 FA Cybersecurity Threat Landscape

Malicious cyber actors continue to target the California food and agriculture sector[2]; most of these attacks seek financial gain. However, it is possible for state-sponsored cyber espionage actors to target the industry to defend their economic interests by seeking information related to business operations and to steal new processes and technologies. Ransomware will remain a prevalent threat while cyber espionage is a lower threat to California-based entities. Given the history of poor security practices within many newly developed cyber-physical industries, it is likely that the food and agriculture sector is relatively unprepared to respond to cyber threats. Furthermore, there are likely to be many vulnerabilities for threat actors to exploit.

2.3 Scale of California's W&WW Sector

There are approximately 8,205 public water systems in California. The California State Water Boards defines public water system as a system for the provision of water for human consumption through pipes or other constructed conveyances that has 15 or more service connections or regularly serves at least 25 individuals daily at least 60 days out of the year. Other public water systems can include

[1] https://www.cdfa.ca.gov/Statistics/PDFs/2022_Ag_Stats_Review.pdf
[2] CAL-CS IC-202007-003

businesses, churches, schools, restaurants, rest stops, and other similar establishments.[3]

Tangentially, wastewater management includes wastewater collection, conveyance, treatment, reuse, and disposal. According to the Water Education Foundation, roughly 4 billion gallons of wastewater is generated in California, daily. Wastewater is moved through approximately 100,000 miles of sanitary sewer lines and treated at more than 900 wastewater treatment plants. There are approximately 6,000 active certified wastewater treatment plant operators throughout California.[4]

Lastly, a community water system (CWS) is defined as a public water system that serves at least 15 service connections used by yearlong residents or regularly serves at least 25 yearlong residents of the area served by the system. There are approximately 2,856 CWSs in California.[5] While the largest public water systems in the state bear the most risk due to their higher levels of exposure and the severity an impact could have, smaller to medium-sized water systems tend to be more vulnerable because they lack the resources their larger counterparts have, leading to a potential increase in the probability of an effective attack.

2.4 W&WW Cybersecurity Threat Landscape

The Cal-CSIC produced an intelligence analysis that assessed[6] that cyberattacks present a threat to the California Water and Wastewater sector. These sectors are critical services to the general public and the other critical infrastructure sectors, some of which are dependent upon these services to conduct their operations but exhibit numerous cybersecurity weaknesses. This is further exacerbated by their slower cybersecurity maturity. The W&WW industry may be less mature as there are many smaller, disparate systems, making W&WW far more fractured in its governance of cybersecurity than the other critical infrastructure sectors. This is intensified by the rising skill-level of threat actors and the lowering of the bar in targeting W&WW operational technology (OT) networks.

[3] Information provided by California State Water Boards
[4] Information provided by California State Water Boards
[5] Information provided by California State Water Boards
[6] CAL-CSIC-202202-004

3 Goal Of the Outreach Plan

The goal of the multi-year outreach plan is to identify, prioritize, and conduct strategic outreach to those entities which have the greatest impact to the State of California. Moreover, through the execution of this plan, the Cal-CSIC seeks to measurably improve cybersecurity in the FA and W&W sectors through a mixture of cybersecurity education, awareness, and improved access to resources.

3.1 Strategic, Multiyear Outreach Plan

In order to develop and execute this plan, the Cal-CSIC continues to engage two categories of outreach; initial outreach activities and tailored, risk-based focused outreach. In the implementation of this strategic, multiyear plan, the Cal-CSIC will move from a broad-based outreach approach of providing general information and assistance to all stakeholders toward a shorter, targeted list based on application of a risk management framework.

However, the Cal-CSIC must ensure the focus is on the correct critical infrastructure sector level of organization (e.g., sector, sub-sector, segment, or sub-segment) or on an organization that crosses all levels of organization, such as non-profit organization that focuses on a particular sector and has stakeholders from each level of organization.

This risk-based and focused outreach will consider: criticality within these sectors, degree of cyber domain exposure, the threat landscape as it relates to these sectors, interrelationships between stakeholders, and economic factors. As noted earlier, DHS provides a tool for understanding this complexity, the infrastructure Data Taxonomy. This is invaluable in understanding the magnitude of the outreach task at hand. Moreover, it demonstrated the need for tailored information and assistance to the specific cybersecurity needs of critical players within each sector.

In the development of this plan, it became clear that taking a risk-based approach to each sector and identifying sector-specific critical functions will lead to a manageable, focused list of stakeholders. This risk-based approach will also prioritize the most effective and important types of information and assistance to provide. This risk-based approach is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework[7].

The Multi-Year Outreach Plan is outlined below into three phases over an estimated four years. Although phase 1 is complete, it is important to note that

[7] https://www.nist.gov/cyberframework

this is a projected timeline and subsequent phases may require additional flexibility pending analytical findings.

- YEAR 1: Phase 1: Research and Limited Outreach – Initial Plan
- YEAR 2: Phase 2: Prioritization and Scoping
- YEAR 3: Phase 2: Part 2: Prioritization and Scoping
- YEAR 4: Phase 3: Proceed to Risk-Informed, Tailored Outreach

3.2 Descriptions of Phase By Year

YEAR 1: Phase 1: Research and Limited Outreach

Initial outreach has been completed, guiding the Cal-CSIC's development of this plan. This phase involved initial scoping of the problem and using existing resources to develop a tentative plan and is now complete as described in this report. This tentative initial plan outlines major efforts, with the expectation of additional refinement and details as the multi-year plan unfolds. The plan will leverage existing state resources within Cal OES, specifically its Homeland Security Division (HSD) State Threat Assessment Center (STAC) Critical Infrastructure Protection (CIP) team, Cal-CSIC's Cybersecurity Task Force (CTF), along with other state agencies and federal partners, including the Department of Homeland Security/Cybersecurity & Infrastructure Security Agency (CISA). Planning efforts thus far revealed the complexity of outreach and that the Cal-CSIC will require an additional two years for Prioritization and Scoping in order to achieve our goal to be the most impactful in our outreach efforts.

YEAR 2: Phase 2: Prioritization and Scoping

This prioritization and scoping phase will be separated into two parts. Goal completion of phase two is projected to span approximately two years. However, initial findings in Phase 2 may change the outlined timeline.

- Part 1: Apply Risk Management Framework
  - Step 1: Defining Objectives
  - Step 2: Identify Organizations
  - Step 3: Organization Analysis
- Part 2: See Year 3

Phase 2, Part 1, Step 1: Defining Objectives

To begin the "Prioritization and Scoping Phase," the Cal-CSIC will develop and designate objectives, lines of effort (LoE) to achieve established objectives, and measures of success (MoS) to demonstrate achievement. The objectives listed here are not listed with any particular order, with the exception of Objective 1 of

the plan. Rather, objectives within this phase are interrelated and interdependent, therefore elements of all three will continue throughout the execution of this plan.

The objectives are:

- **Objective 1:** Develop multiyear outreach plan to assist the FA and W&WW sectors in their efforts to improve cybersecurity;
- **Objective 2:** Increase preparedness and awareness to reduce the likelihood and severity of cybersecurity incidents; and
- **Objective 3:** Promote reporting when a significant and verified threat is identified (cybersecurity incidents) or an attack is underway.

To achieve these objectives, the Cal-CSIC will utilize the following concurrent Lines of Effort:

- LoE 1: Organizational Analysis
- LoE 2: Communications
- LoE 3: Resource Acquisition Efforts
- LoE 4: Measuring

Discussion of these LoEs and the MoS can be found below in the section "Plan to Evaluate Success of Outreach Plan."

Phase 2, Part 1, Step 2: Identifying Organizations

The Cal-CSIC has developed an initial list of potential organizations. However, the Cal-CSIC will determine the full list of sector-specific organizations and key stakeholders in each of those sectors during Phase 2. This list will be informed and prioritized by sector cybersecurity risk analysis. Stakeholder Organizations will be approached by grouping/prioritizing the organizations based on greatest impact to the State of California, its citizens, overall economy, and cybersecurity risk rating. As noted previously, an analysis of this magnitude will require assistance from partner organizations, such as the STAC CIP team, and/or non-governmental organizations (NGO) with subject matter expertise in aforementioned sectors. Not every sub-sector or organization will necessarily have a significant cybersecurity role – this will depend on the degree of automation and information technology dependencies in that area.

Sector specific agencies and partners may be able to provide more extensive data and sector-specific analytical support in these areas. In turn, this data may be used to make better informed decisions. During Phase 1, the Cal-CSIC identified nearly 600 FA nonprofits in California and multiple sources list nearly 50 organizations involved in water issues. To ensure efficacy, the plan must address organizations with the highest risk most significance and filter down using a

methodology developed in the Prioritize and Scope phase, informed by the sector analysis described above.

The Cal-CSIC will coordinate with Cal-CSIC Cyber Threat Intelligence (CTI) and STAC CIP teams to receive a "top 10" list to prioritize organizations based on physical infrastructure. The Cal OES CIP team, with the help of partner agencies at the federal, state, and non-governmental level, may be able to determine where there is an information technology and operational technology (IT/OT) convergence in critical infrastructure. Furthermore, through this collaboration, an understanding of how the loss of said infrastructure would have a trickledown effect on the cyber domain if its availability were degraded may be better understood. This process would begin by applying a risk methodology, specifically MSHARRPP+V[8], developed for physical infrastructure. However, this methodology will need to be adapted to the cyber domain, as informed by the NIST Cybersecurity Framework. Further, CTI can assist in illuminating, prioritizing, and addressing risks from threats to these critical infrastructure sectors. This will create a feedback loop to aid the CTI Branch in providing relevant and timely cyber threat intelligence to key stakeholders within each sector

Protecting these two sectors of critical infrastructure is a strategic interest shared by federal, state, local, tribal, and territorial governments, and private sector partners. Interruption of operations within them could have a devastating impact on the Nation's public health and economy. The security and resilience of infrastructure in both sectors requires all sector partners to undertake several integrated processes and procedures.

Phase 2, Part 1, Step 3: Organization Analysis

To identify key organizations, points of contact, prioritization methodologies, and the critical domain-specific knowledge associated with each sector, the Cal-CSIC will need to rely heavily on partners with subject matter expertise. Additionally, the Cal-CSIC will build on previously established partnerships with the California Department of Food and Agriculture (CDFA) and the relevant water boards, expanding that partnership to other relevant state agencies. During the planning phase the Cal-CSIC met with emergency management and cybersecurity personnel from various agencies to understand the breadth of these sectors. Additionally, discussions surrounding cybersecurity challenges unique to these sectors, and additional stakeholders to consider for additional outreach were conducted. The Cal-CSIC will follow up to further clarify and prioritize these lists. The Cal-CSIC will need to gather information about prioritized organizations through network owners and partner organizations.

[8] Cal OES STAC CIP uses a methodology from the DHS ACAMS program known as MSHARRPP+V. The abbreviation stands for Mission, Symbolism, History, Accessibility, Recognizability, Recoverability, Population, Proximity and Vulnerability.

Information gained can then be analyzed to better understand their specific business drivers, interests, and communication preferences. Ultimately, this will tailor nearly all outreach efforts.

Each infrastructure sector and their respective subsectors have their own unique set of OT[9], widely varying degrees of information technology application and sophistication, different stakeholder groups and organizations, different industries and economies, and different cultures. This requires enlisting the assistance of subject matter experts in many or most of these different areas, most of whom are outside government.

Further, the FA sector is almost entirely under private ownership. A different approach than that used with government agencies would be necessary to conduct a thorough study of this vast sector to determine which farms (and related businesses) to prioritize as most critical. NGOs and trade associations will play a significant role in this aspect of the outreach.

Additionally, the FA sector is critically dependent on the W&WW sector for clean irrigation and processed water. Likewise, FA and W&WW have dependencies in other critical infrastructure sectors. The transportation sector is necessary for movement of products and livestock. The energy sector provides power to the equipment needed for agriculture production and food processing. The chemical sector provides fertilizers and pesticides used in crop production. The interdependence of these systems illustrates the magnitude and complexity of planning outreach and must be considered in any critical systems analysis.

Appropriate prioritization is a major factor in this analysis and very important to get right. It is necessary to narrow the scope of outreach to the most important areas to ensure efficient resource utilization and allocation. It is possible various entities have already done research at a statewide-level or with a California focus that resulted in such prioritization but finding that research also requires significant collaborative work to locate and evaluate.

Finally, the Cal-CSIC analysis will consider threats which exist in the boundary region between the cyber and physical domain, otherwise known as cyber/physical threats. For example, physical attacks which cause cyber effects or cyberattacks which cause physical effects. This is an area that requires the combined expertise of the Cal-CSIC and the STAC CIP along with other partners.

[9] Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.

YEAR 3: Phase 2, Part 2: Complete Prioritization and Scoping

During this phase prioritization and scoping should be completed. Nevertheless, pending initial outcomes of Phase 2 Part 1, the timeframe may need to be adjusted.

Complete Prioritization and Scoping: use applied risk management framework results to focus efforts on greatest need, greatest risk

- Create a Content Calendars
- Finalize Refined Plan

Following Phase 2 Part 1, the Cal-CSIC will develop content calendars. Each calendar will be specific to the identified level of organization, outlining the timing, frequency, and theme for outreach activities. Consideration for these activities will be made based on previous Prioritization and Scoping Phase analysis, specific to each sector. This will allow for consistent messaging and proactive planning of content creation and distribution and will increase the likelihood that MoS are effectively communicated and methodically analyzed.

YEAR 4: Phase 3: Proceed to Risk-Informed, Tailored Outreach

Targeted outreach will begin when the Cal-CSIC has completed the Prioritization and Scoping Phase. Outreach activities will become more risk-informed and tailored to these sectors and the entities within them.

The initial strategic messaging is critical and will require the Cal-CSIC to send clear and concise messages aligning with Cal-CSIC's objectives. Additionally, this messaging should include input from key stakeholders, which will be determined during the Prioritization and Scoping Phase. The identification of a 'change champion' within each sector will aid in the dissemination of information, specific to each sector. Working with relevant stakeholders and/or organizations who can help amplify Cal-CSIC's message and expand outreach efforts will be critical. A trusted messaging partner can lead to enhanced credibility and extend our reach for communication. Such stakeholders include, but are not limited to, CDFA, the relevant state and federal water boards, the California Department of Health and Human Services (Cal-HHS), California Highway Patrol (CHP), California Department of Technology (CDT), Department of Justice (DOJ), and the California Military Department (CMD) and the multitude of NGOs that are critical to representing these diverse and complex critical infrastructure sectors.

Tailored messaging will provide warnings of cyberattacks, coordinate information sharing, assess risks to critical infrastructure information networks, enable cross-sector coordination, and sharing of best practices and security

measures, and support certain cybersecurity assessments, audits, and accountability programs.

4 Methods For Coordinating with Partners

Coordination with partners will continue through Phase 2 and into Phase 3. As effective coordination should be risk-based, this will evolve as the Risk Management Framework is applied.

The Cal-CSIC will follow through with the outreach plan via established communication channels and deliver messages to stakeholder organizations. The level of engagement will be determined during coordination and collaboration events but may range in scale. Engagement will start from something as simple as mass emails and newsletters but then expand to surveys, self-help tools, virtual workshops, and seminars/webinars, "train the trainer" sessions, public meetings, blog posts or maybe videos. Where use of social media is appropriate, it can be used to engage the Cal-CSIC's target audience at lesser cost and impact to all partners and stakeholders. For instance, creating compelling and sharable content, encouraging organizations' interactions, and promptly responding to queries and/or comments can all greatly expand the reach of the Cal-CSIC's cybersecurity messaging.

5 Estimate Of Funding

Resource	Cost	Details
Estimated Cal-CSIC Staff Workload	$270,000 x 3 PY = $810,000 (annual)	This is a moderate-confidence estimate based on current average personnel costs and estimated workload
External Consulting Contract	$2,000,000 (one-time)	This is a moderate-confidence estimate based on previous consulting contracts
Total:	$810,000 annually $2,000,000 one-time	

In order to effectively implement this plan, the Cal-CSIC and its Lead Cyber Policy and Strategy Planner will require additional resources including technical expertise from Cal OES Homeland Security Division's Critical Infrastructure

Program (CIP). While funding was previously provided for development of the plan, based on a rough analysis, the ongoing outreach effort requires $810,000 annually and an additional $2,000,000 one-time for an external consulting contract.

Due to the complexity and timeliness of this project, Cal-CSIC's recommendation is to pursue an external consultation contract to supplement currently funded staff.

6 Potential Funding Sources for Outreach Plan

Potential Funding Source	Budgeted or Allocated Amount
State and Local Cybersecurity Grant Program (SLCGP)	Federal FY22: some likely small fraction of $7,577,949[10] (depends on Cybersecurity Plan alignment and grantee applications received and approved) Federal FY23: TBD Federal FY24: TBD Federal FY25: TBD

7 Plan To Evaluate Success of Outreach Plan

The Cal-CSIC will maintain regular communication with sector stakeholders. Such communication may include providing them with updates, conducting surveys, responding to their inquiries, and proactively sharing relevant information to foster ongoing engagement.

The Cal-CSIC will focus on the following Measures of Success (MoS). Similar to the objectives, the MoS are not ordered necessarily by importance or chronologically, as they overlap and are interdependent. Additionally, the MoS should be considered flexible as the Cal-CSIC, and its partners begin to grasp the needs of each sector as it relates to cybersecurity.

- **MoS 1:** Increase awareness regarding the importance of cybersecurity;
- **MoS 2:** Reduce the frequency, severity, and impact of cyberattacks against the FA and W&WW sectors;
- **MoS 3:** Reduce entity cybersecurity risk and increase the safety and integrity of food and water and related systems;
- **MoS 4:** Avoid supply chain delays caused by cyberattacks which would drive increased food costs and food insecurity;
- **MoS 5:** Avoid putting personal or proprietary information at risk.

[10] Represents 95% of total federal award as 5% is allocated to Management and Administration

The MoS will be further refined and solidified during the Prioritization and Scoping Phase with empirical data. The following Key Performance Indicators (KPI) will enable more precise and meaningful results:

- **KPI 1:** Increase of Cal-CSIC Cyber Threat Intelligence (CTI) Branch monitoring of FA and W&WW sectors [aligns to MoS 1, 2, 3, 4, 5]
- **KPI 2:** Establishment of quantifiable sector-specific incident metrics provided by CTI Branch [aligns to MoS 1, 2, 3]
- **KPI 3:** Increase of FA and W&WW subscriptions to CTI threat intelligence distribution list [aligns to MoS 1, 2, 3, 4]
- **KPI 4:** Increase of CTI threat intelligence production specific to FA and W&WW sectors [aligns to MoS 1, 2, 3, 4]
- **KPI 5:** Reductions in FA and W&WW incident rates, severity, and impact (as percentage of entities monitored) [aligns to MoS 1, 2, 3, 4]
- **KPI 6:** Reduction in alerts generated during active network monitoring (as percentage of sector entities enrolled in CDT or Cal-CSIC services) [aligns to MoS 1, 2, 3]
- **KPI 7:** Increase in FA and W&WW requests for proactive Cal-CSIC services [aligns to MoS 1, 2, 3, 4]
- **KPI 8:** Increase in applicable grant requests from FA and W&WW [aligns to MoS 1, 2, 3]
- **KPI 9:** Increase in grant funds distributed to FA and W&WW [aligns to MoS 1, 2, 3]
- **KPI 10:** Increase in training requests from FA and W&WW [aligns to MoS 1, 2, 3, 4]
- **KPI 11:** Increase in Cal-CSIC media engagements related to FA and W&WW [aligns to MoS 4]
- **KPI 12:** Increased requests for CDT or Cal-CSIC services for FA and W&WW [aligns to MoS 1, 2, 3, 4]
- **KPI 13:** Increased FA and W&WW enrollment in and completion of no-cost services provided or facilitated by CISA[11] [aligns to MoS 1, 2, 3, 4]

To enable this effort, all these metrics will need to be baselined at the beginning of Phase 2, and this list will be revised as necessary where data is unavailable or impractical to track.

[11] https://www.cisa.gov/stopransomware/services

8 Evaluation Of Grants or Alternative Forms of Funding to Improve Cybersecurity Preparedness

8.1 Summary Of Evaluation Performed by Cal-CSIC

The Cal-CSIC coordinated with the California Department of Food and Agriculture (CDFA) and California Water Boards (Waterboards) to review all available grant programs which were aligned with cybersecurity preparedness. Additionally, we sought assistance from the Cal-OES Grants Unit to evaluate options for providing grants or alternative forms of funding. Cal-OES Grants evaluated all available grants of which the agency acts as a recipient or provides pass through funding to subrecipients. Currently, the Cal-CSIC is directly involved with two grant programs, the State and Local Cybersecurity Grant Program (SLCGP) and the Homeland Security Grant Program (HSGP). These two programs may be helpful to the FA and W&WW sectors and to Cal-OES in executing this plan. Additional federal grant programs or funding sources that may be applicable is described in the following section. During the Prioritization and Scoping Phase, the Cal-CSIC will continue to seek and identify other plausible funding sources for these sectors and will raise awareness of these programs in those sectors.

8.2 Listing Of Funding Sources (Grants or Alternatives) for Improved Cybersecurity Preparedness

State and Local Cybersecurity Grant Program

The SLCGP provides funds to improve the cybersecurity of state, tribal, and local governments including that of critical infrastructure. The primary focus of the program is on local governments and rural populations. The program requires at least 80% of funds go to local governments and 25% to rural communities. While the FA and W&WW sectors are not specifically named in this program, potential subrecipients include those which may be within these sectors if they are government entities or instrumentalities of governments like special districts for example.[12]

In its first year (Federal FY22), California was awarded $7,976,788 in SLCGP funding. Yet, until all sub-recipient applications are received and processed Cal OES is unable to estimate the portion of those funds going to the FA and W&WW sectors. In the second year (Federal FY23), $15,879,497 was allocated to

[12] https://www.caloes.ca.gov/SLCGP

California. Once more, at the time of this report, the portion to be allocated to FA and W&WW sectors is not yet known. California is expected to receive approximately $11 million (FY24) and $3 million (FY25) under SLCGP, but the exact amount will not be known until published by FEMA.

W&WW and Cybersecurity Grants

The following grants are specific to cybersecurity in the W&WW critical infrastructure sector.

Water Technical Assistance Programs

This grant is administered by United States Environmental Protection Agency (US EPA)[13] [14] and offers online and in-person courses on water sector cybersecurity threats, vulnerabilities, consequences, best practices, resources, and program development.

Clean Water State Revolving Fund (CWSRF)

The CWSRF, capitalized by the US EPA and administered by the State Water Resources Control Board, is authorized to provide assistance with All-Hazard Risk and Resilience Assessment, Training, Equipment, and Infrastructure, including cybersecurity[15]. Eligibility may vary based on the current years Intended Use Plan adopted by the State Water Boards[16].

Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program

This US EPA grant program assists medium and large size public water systems with protecting drinking water sources from natural hazards, extreme weather events, and cybersecurity threats[17].

Rural and Municipal Utility Advances Cybersecurity Grant and Technical Assistance Program

This United States Department of Energy (DOE) grant program is designed to provide technical assistance to eligible entities to protect against, detect,

[13] https://www.epa.gov/ground-water-and-drinking-water/drinking-water-grants
[14] https://www.epa.gov/water-infrastructure/water-technical-assistance-programs
[15] https://www.epa.gov/waterresilience/cybersecurity-funding
[16] https://www.waterboards.ca.gov/water_issues/programs/grants_loans/srf/
[17] https://www.epa.gov/dwcapacity/midsize-and-large-drinking-water-system-infrastructure-resilience-and-sustainability

respond to, and recover from cybersecurity threats. This includes utilities that provide both water and electricity[18].

USDA-RD Circuit Rider Program - Technical Assistance for Rural Water Systems

This program is administered by the United States Department of Agriculture (US DA) and provides technical assistance to rural water systems that are experiencing day-to-day operational, financial or managerial issues. One of the listed topics with which the Circuit Rider can assist is security. A system may request assistance from the National Rural Water Association State Association or the local Rural Utilities Service office[19].

Other Additional Grant Programs

The following grant programs are not cybersecurity nor sector specific, however, could potentially be utilized.

Homeland Security Grant Program

The HSGP contains a cybersecurity provision that could potentially benefit the FA and W&WW sectors. Generally, projects which will "enhance cybersecurity" are authorized for funding under this program. More specifically, these would be projects "that would aid in implementation of all, or part of the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework") developed by the NIST.[20] But applications tied to this provision would compete with other non-cybersecurity proposals.

Nonprofit Security Grant Program (NSGP)

The NSGP maintains cybersecurity provisions. "The objective of the FY 2023 NSGP is to provide funding for physical and cybersecurity enhancements."[21] This includes funding for training on "topics are limited to the protection of critical infrastructure key resources, including physical and cybersecurity…" This may be of more benefit to the FA sector where a multitude of NGOs exist. [22] The

---

[18] https://www.energy.gov/ceser/rural-and-municipal-utility-advances-cybersecurity-grant-and-technical-assistance-program
[19] https://www.rd.usda.gov/programs-services/water-environmental-programs/circuit-rider-program-technical-assistance-rural-water-systems
[20] https://www.fema.gov/sites/default/files/documents/fema_gpd-fy-23-preparedness-grants-manual.pdf
[21] https://www.fema.gov/grants/preparedness/nonprofit-security/fy-23-nofo
[22] https://www.fema.gov/sites/default/files/documents/fema_gpd-fy-23-preparedness-grants-manual.pdf

California State Nonprofit Security Grant Program mirrors the federal NSGP but is funded by state general funds.[23]

Port Security Grant Program (PSGP)

The PSGP has some areas of overlap with the FA and W&WW sectors and also includes a cybersecurity provision. PSGP funds may be used for projects that enhance the cybersecurity of numerous port facility systems. [24]

8.3 Potential Voluntary Actions

The Cal-CSIC and partner organizations may work with network owners in determining the best methods to carry out the outreach and assistance plans. This may include voluntary actions, awareness, and potentially, resource acquisition.

However, in the general sense, there are best practices, such as implementing NIST frameworks or CISA guidelines, that can be implemented to increase cybersecurity. These methods can be provided through outreach, training, and awareness campaigns. Additionally, network owners may will benefit from open communications with partners. Voluntary reporting of cybersecurity incidents can increase network owners' access to resources and assistance.

The Cal-CSIC will strongly advise that all network owners coordinate with and participate in activities through a multitude of available outreach channels. These channels contain several state and local government partner organizations, to include, but not limited to:

- California Cybersecurity Task Force
- California Cybersecurity Task Force Critical Infrastructure Subcommittee
- Cal-CSIC Cyber Threat Intelligence Branch (free subscription service)
- Cal-CSIC Operations Branch incident reporting program
- Cal-CSIC Operations Branch incident response program
- Cal OES Homeland Security Division STAC CIP
- Cybersecurity and Infrastructure Security Agency (CISA)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Water Information Sharing and Analysis Center (WaterISAC)
- Municipal Information Systems Association of California (MISAC)
- California County Information Services Directors Association (CCISDA)

---

[23] https://www.caloes.ca.gov/office-of-the-director/policy-administration/finance-administration/grants-management/homeland-security-emergency-management-programs/infrastructure-protection-grants/

[24] https://www.fema.gov/sites/default/files/documents/fema_gpd-fy-23-preparedness-grants-manual.pdf

9 Conclusion

Through development of this plan the Cal-CSIC found that the FA and W&WW critical infrastructure sectors are extremely complex systems. Furthermore, these sectors require considerable time and resources to account for their sector-specific risk and the actionable cybersecurity measures that would reduce that risk through outreach. The Cal-CSIC has taken a risk-based approach to scoping and prioritization of the plan which is limited to current Cal-CSIC resources. This plan is meant to be dynamic and flexible and may require updates as the Cal-CSIC gains additional information and phases are completed. The Cal-CSIC's plan will require committed efforts from the State, partner departments and agencies, and the individual entities that comprise each sector to effectively achieve all objectives.