Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

California State & Local Cybersecurity Grant Program (SLCGP)

Update: October 6, 2023

California Governor's Office of Emergency Services
California Cybersecurity Integration Center (Cal-CSIC)

California SLCGP Background, continued

- **Eligible <u>Recipient</u>**:
  - Governor-designated **State Administrative Agency (SAA) - OES is SAA for California**
- <u>**Sub-Recipients** – state agencies and "local governments" (see sidebar)</u>:
  - **80% will be passed through** (directly or via in-kind services) to local governments
  - **25% of total must go to "rural"** areas/jurisdictions (less than 50k population)
- **Award use**: Planning; Equipment; Exercises; Management & Administration (M&A); Organization; Training
- **Cybersecurity Planning Committee**: responsible for producing and approving the Cybersecurity Plan
- **Cybersecurity Plan**: addresses requirements in NOFO and determines funding allocations – approved for CA by DHS/FEMA/CISA Sept. 2023
- **Cost share requirements:**
  - **10% in FY22 – Cal OES submitted waiver request, approved by FEMA**
  - **20% in FY23, 30% FY24, 40% FY25** – must use non-federal funds
  - **Hard match** is non-federal cash spent for project-related costs such as state or local general funds monies; ***Soft Match*** (in-kind) includes services in lieu of cash which benefit program such as work toward cybersecurity plan, gap analysis, local-level grant M&A
- **Period of Performance**: 48 months per FY award (12/1/2022 to 11/30/2026 for FY22 award, projected to be 12/1/2023 to 11/30/2027 for FY23 funds)

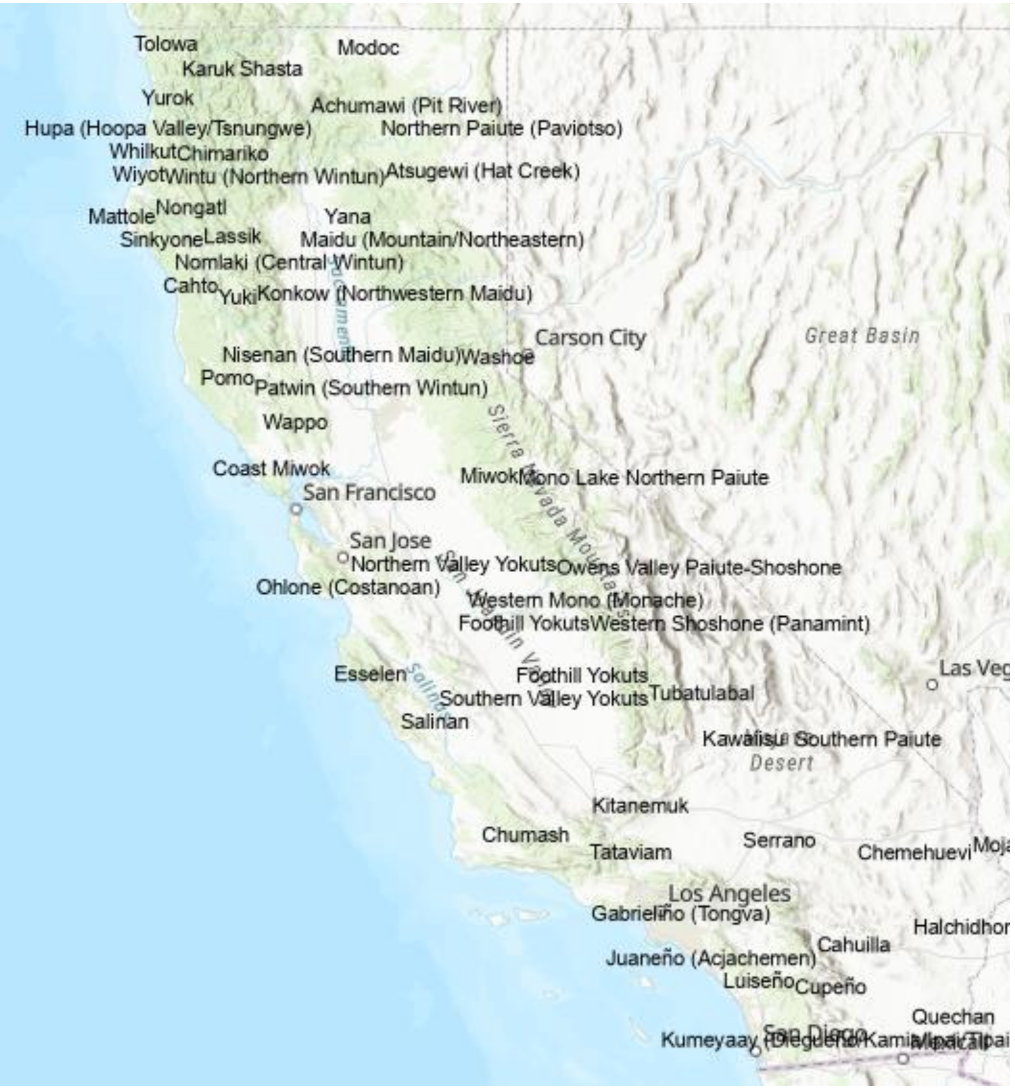
"Local government" is defined in 6 U.S.C. § 101(13) as:

A) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regional or interstate government entity, or agency or instrumentality of a local government;

B) An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

C) A rural community, unincorporated town or village, or other public entity.

Tribal Cybersecurity Grant Program (TCGP)

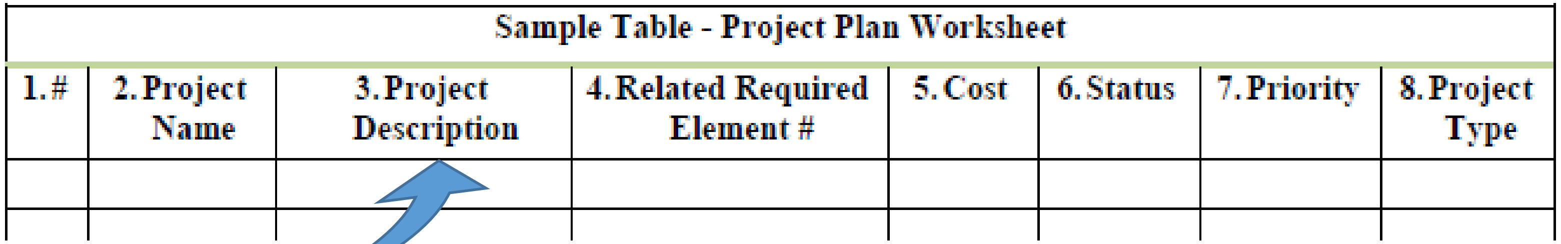


- Tribal Cybersecurity Grant Program (TCGP) **NOFO announced September 27, 2023:**
  - https://www.cisa.gov/news-events/news/cisa-and-fema-open-application-process-tribal-cybersecurity-grant-program
- Like SLCGP, **helps eligible entities address cybersecurity risks and threats to information systems owned or operated by or on behalf of Tribal governments**
- Tribal governments have **options**:
  - Apply to SLCGP through State Administrative Agency (SAA) – **Cal OES**
  - Apply to TCGP **directly to FEMA**
  - Apply to **both**
- **Tribal governments should contact CISA and/or FEMA directly regarding TCGP: FEMA-TCGP@fema.dhs.gov**

California SLCGP Update

- OES/Cal-CSIC **SLCGP project management team** has been working constantly since August 2022 to plan and organize grant applications, planning committee formation, cybersecurity plan development and submission; has been meeting with CISA, FEMA to update status, clarify requirements
- Completed **capability gap survey** (May 2023) **analysis** (May-July 2023), **preferred services survey** (Aug-Sep 2023) representing all potential sub-recipient groups (counties, cities, special districts, tribal gov't, state gov't) including input from working groups; combined with CISA/NIST **risk analysis framework drove prioritization of focus areas**
- "**Projects**" that must be listed and summarized in Plan are categorical, essentially *lines of effort* or *focus areas* – details will be identified in subsequent Investment Justifications for each project

Column 3. Brief (e.g., 1-line) Description of the purpose of the project

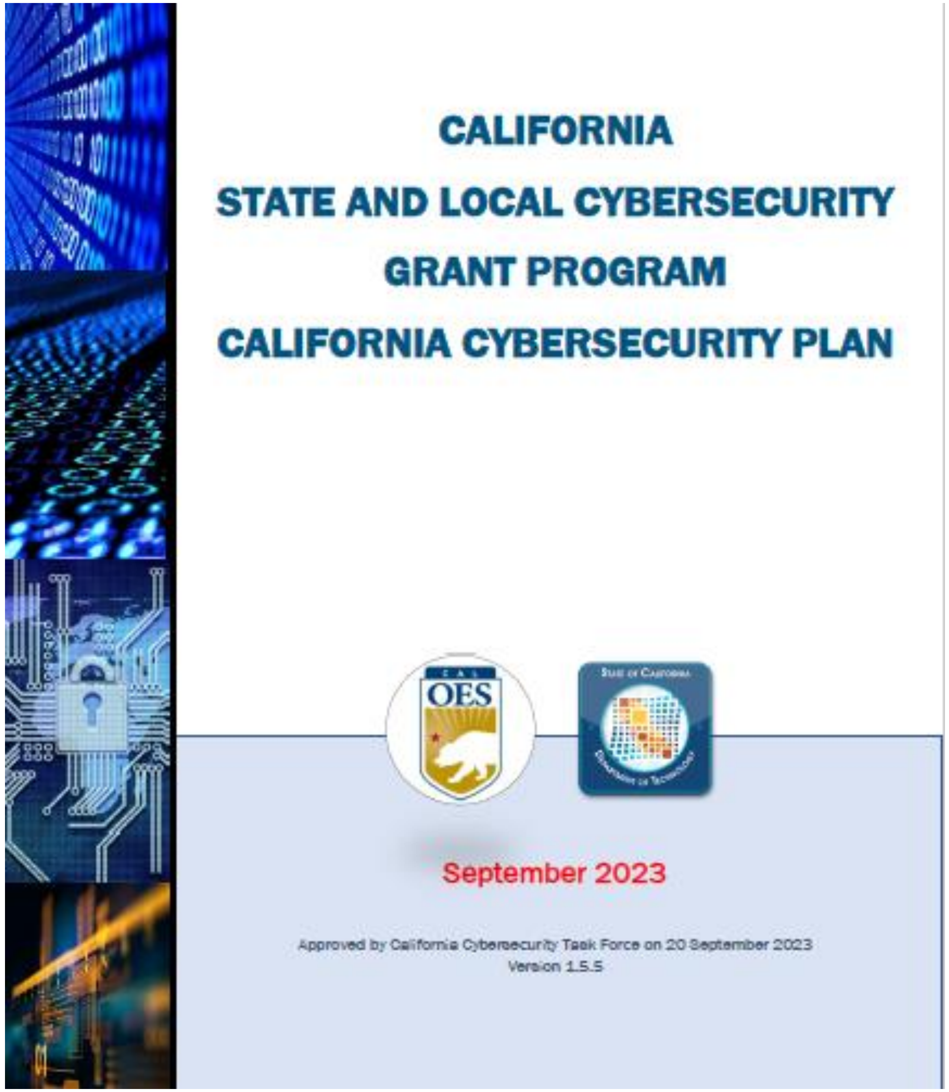


Sample Table - Project Plan Worksheet

1.#	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type

California SLCGP Update, continued

- First-year (FY22) grant award of $7.9 million **locked until Cybersecurity Plan approved by CISA/FEMA & individual projects approved (Fall 2023?)**; with exception of 5% to Cal OES for Management and Administration (M&A) allowed by the program
- **2nd year (FY23) allocation to California is $15.9 million**; announced in FY23 NOFO released 7 Aug and Cal OES applied on behalf of state 6 Oct
- CCTF CIPS 100% focused on SLCGP for now; **540+ members**, sending out **regular announcements via email distro**, two information sessions in May 2023
- Cybersecurity Plan **completed by Sept. 30, 2023 due date and approved by DHS/FEMA/CISA!**



CALIFORNIA

STATE AND LOCAL CYBERSECURITY

GRANT PROGRAM

CALIFORNIA CYBERSECURITY PLAN

September 2023

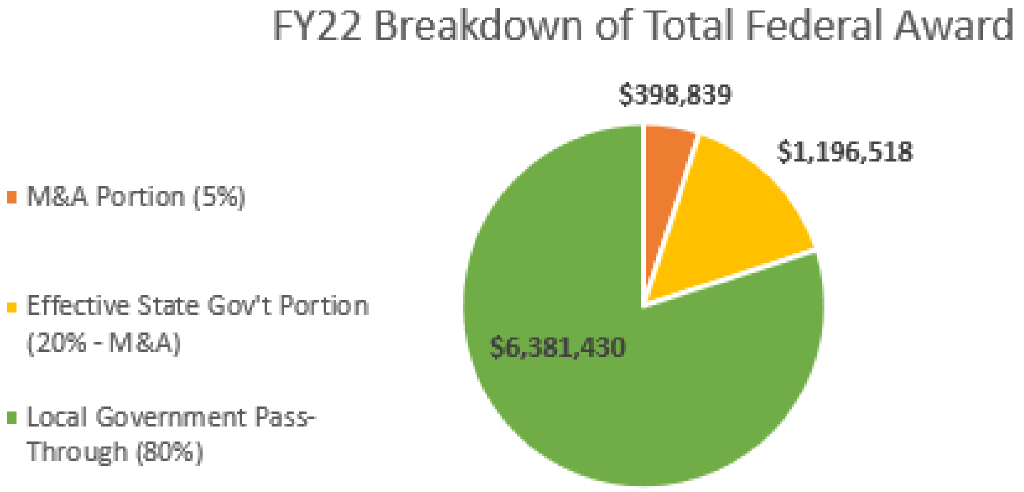
Approved by California Cybersecurity Task Force on 20 September 2023
Version 1.5.5

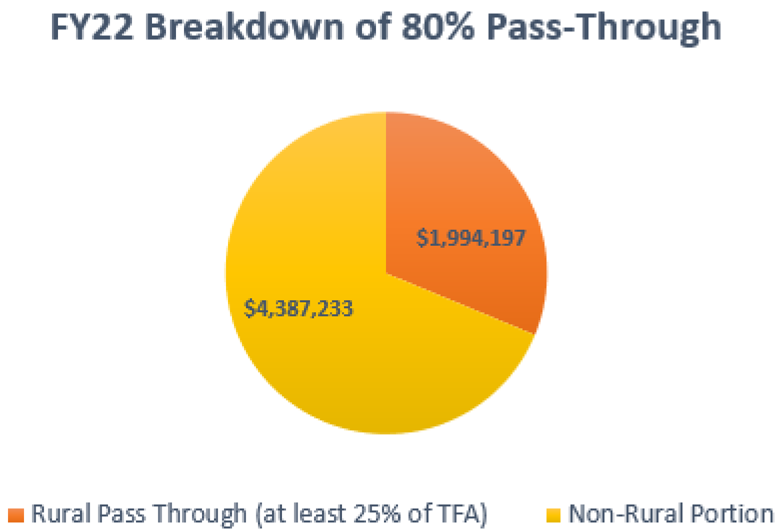
SLCGP Funding Breakdown For California

Period (Fed FY)	Portion	Federal Share	Non-Federal Cost Share %	Non-Federal Cost Share $ (of Total Project Cost)	Total Project Cost Funds (Fed + SLTT shares)	Status
FY22	Total	$7,976,788	10%	WAIVED	$7,976,788	Awarded, non-M&A portion locked
FY22	M&A (5%)	$398,839		WAIVED	$398,839	Being used by project management team, surplus will be re-allocated to state government portion
FY22	Non-M&A (95%)	$7,577,948		WAIVED	$7,577,948	Locked until cybersecurity plan and investment justification/project worksheets approved
FY23	Total	$15,879,497	20%	$3,969,874	$19,849,371	Announced in FY23 NOFO, Cal OES will apply Oct 2023
FY24	Total	$11,909,623 (est.)	30%			TBD, NOFO should be released sometime FY24?
FY25	Total	$3,969,874 (est.)	40%			TBD

SLCGP Funding Breakdown For California, cont'd

Federal Fiscal Year	Nationwide Amount (millions)	Estimate or Actual	California Share (Total Federal Award, actual & estimated)	Cost Share % (of Total Project Cost)	Total Cost Share $ (statewide)	Total Funds (Fed + SLTT shares)	State Gov't Allocation (20%)	M&A Portion (5%)	Effective State Gov't Portion (20% - M&A)	Local Government Pass-Through (80%)	Rural Pass Through (at least 25%)
FY22	200	actual	$7,976,788	0%	$0	$7,976,788	$1,595,358	$398,839	$1,196,518	$6,381,430	$1,994,197
FY23	400	actual	$15,879,497	20%	$3,969,874	$19,849,371	$3,175,899	$793,975	$2,381,925	$12,703,598	$3,969,874
FY24	300	estimate	TBD	30%	TBD	TBD	TBD	TBD	TBD	TBD	TBD
FY25	100	estimate	TBD	40%	TBD	TBD	TBD	TBD	TBD	TBD	TBD
Totals	1000	estimate	TBD		TBD	TBD	TBD	TBD	TBD	TBD	TBD





Funding Models/Options

<u>In-Kind Services (state government as service provider) in lieu of cash:</u>

- Jurisdictions can enroll in services aligned to "projects" → economies of scale
- All applications (enrollees) meeting minimum criteria accepted
- Sub-recipient project proposals <u>not required</u>
- State is establishing cost accounting (cash value of services)
- First-come-first-serve if services at capacity (depends on service costs)

<u>Direct funding to jurisdictions:</u>

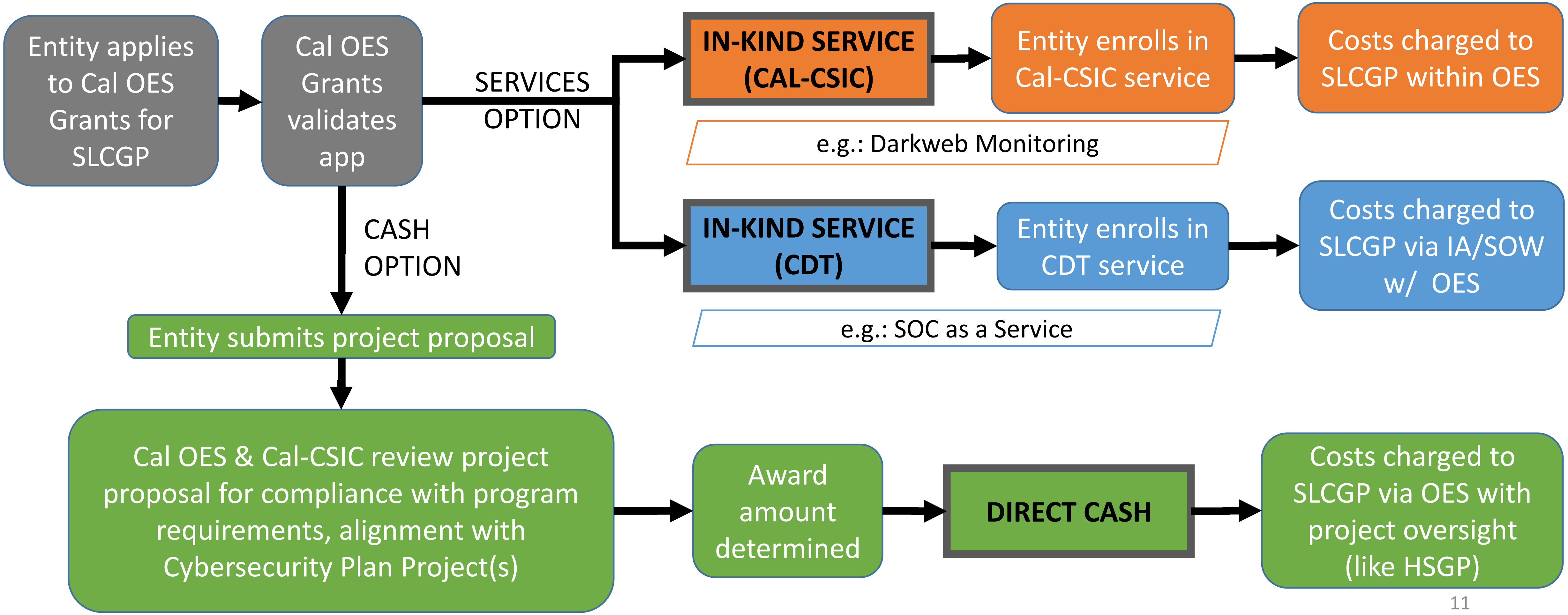
- 80% pass-through (CA is $6,381,430 for FY22, $1,196,518 to state government agencies)
- Jurisdictions must provide complete project proposal that meets same objectives/criteria as one of the projects listed in the approved Cybersecurity Plan
- Will be competitive, scored based on alignment to Cybersecurity Plan

<u>FINAL PLAN → Hybrid/Combination (Services OR Cash):</u>

- The model we settled on, with recommendation/preference for in-kind services
- Default would be in-kind services in lieu of cash; jurisdictions documenting non-consent and opting for cash would need to produce project proposals subject to review

In any case, state must ensure at least 25% (of total) goes to rural, 80% (of total) must pass-through to local governments (whether in-kind services or cash)

California SLCGP Funding Model: Use Cases



Entity applies to Cal OES Grants for SLCGP

Cal OES Grants validates app

SERVICES OPTION

IN-KIND SERVICE (CAL-CSIC)

Entity enrolls in Cal-CSIC service

Costs charged to SLCGP within OES

e.g.: Darkweb Monitoring

IN-KIND SERVICE (CDT)

Entity enrolls in CDT service

Costs charged to SLCGP via IA/SOW w/ OES

e.g.: SOC as a Service

CASH OPTION

Entity submits project proposal

Cal OES & Cal-CSIC review project proposal for compliance with program requirements, alignment with Cybersecurity Plan Project(s)

Award amount determined

DIRECT CASH

Costs charged to SLCGP via OES with project oversight (like HSGP)

16 Required Elements for Cybersecurity Plan

1: Manage, monitor, and track information systems, applications, and user accounts
2: Monitor, audit, and track network traffic and activity
3: Enhance the preparation/response/resiliency of information systems/apps/user accounts
4: Continuous cybersecurity vulnerability assessments/threat mitigation prioritized by risk
5a: Multi-Factor Authentication
5b: Enhanced logging
5c: Data encryption for data at rest and in transit
5d: End use of unsupported/EOL software & hardware accessible from Internet
5e: Prohibit use of known/fixed/default passwords and credentials
5f: Ensure ability to reconstitute systems (backups)
5g: Migration to .gov internet domain
6: Promote delivery of safe/recognizable/trustworthy online services, including .gov
7: Ensure continuity of operations including by conducting exercises
8: Identify/mitigate workforce gaps, enhance recruitment/retention, bolster KSAs (NICE Framework)
9: Ensure continuity of comms & data networks
10: Assess and mitigate, CIKR risks & threats impacting local jurisdictions
11: Share cyber threat indicators with the State of California & DHS
12: Leverage cybersecurity services offered by DHS (CISA)
13: IT/OT modernization cybersecurity review process
14: Develop and coordinate strategies to address cybersecurity risks & threats
15: Ensure rural communities have adequate access to, and participation in plan activities
16: Distribute funds, items, services, capabilities, or activities to local governments/agencies

Guidelines to improve cybersecurity -- must be addressed in plan but NOT conditions for funding!

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

California SLCGP Update, continued

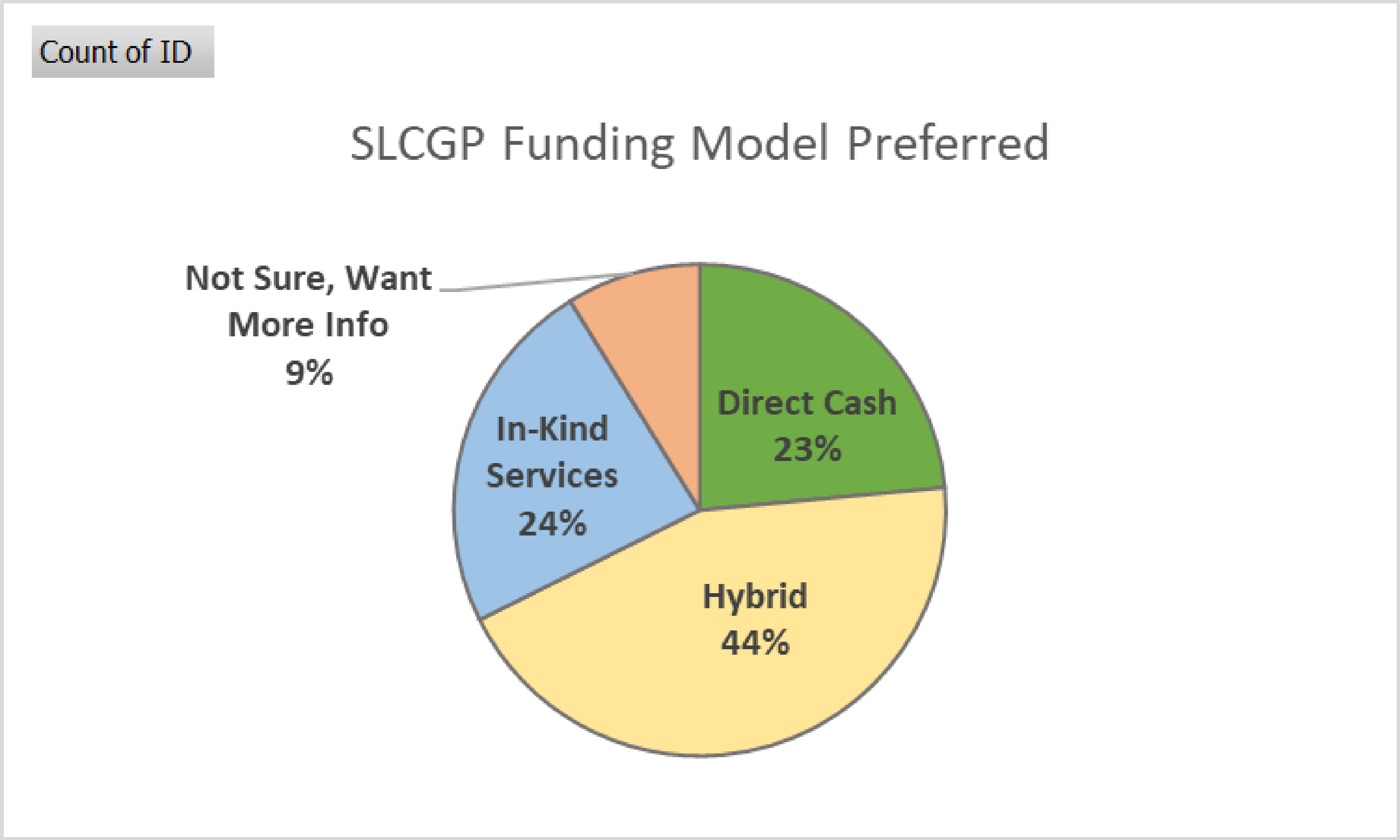
- **<u>SLCGP Statewide Cybersecurity Capability Gap Survey Results</u>**
  - 121 organizations responded across all sectors
  - Combination of multiple choice and short answer questions
  - Columns align with 16 required elements (and sub-elements)
  - Common gaps in planning/organization, exercises, staff resources/training
  - Required step for development of cybersecurity plan; will provide focus/prioritization of "projects"

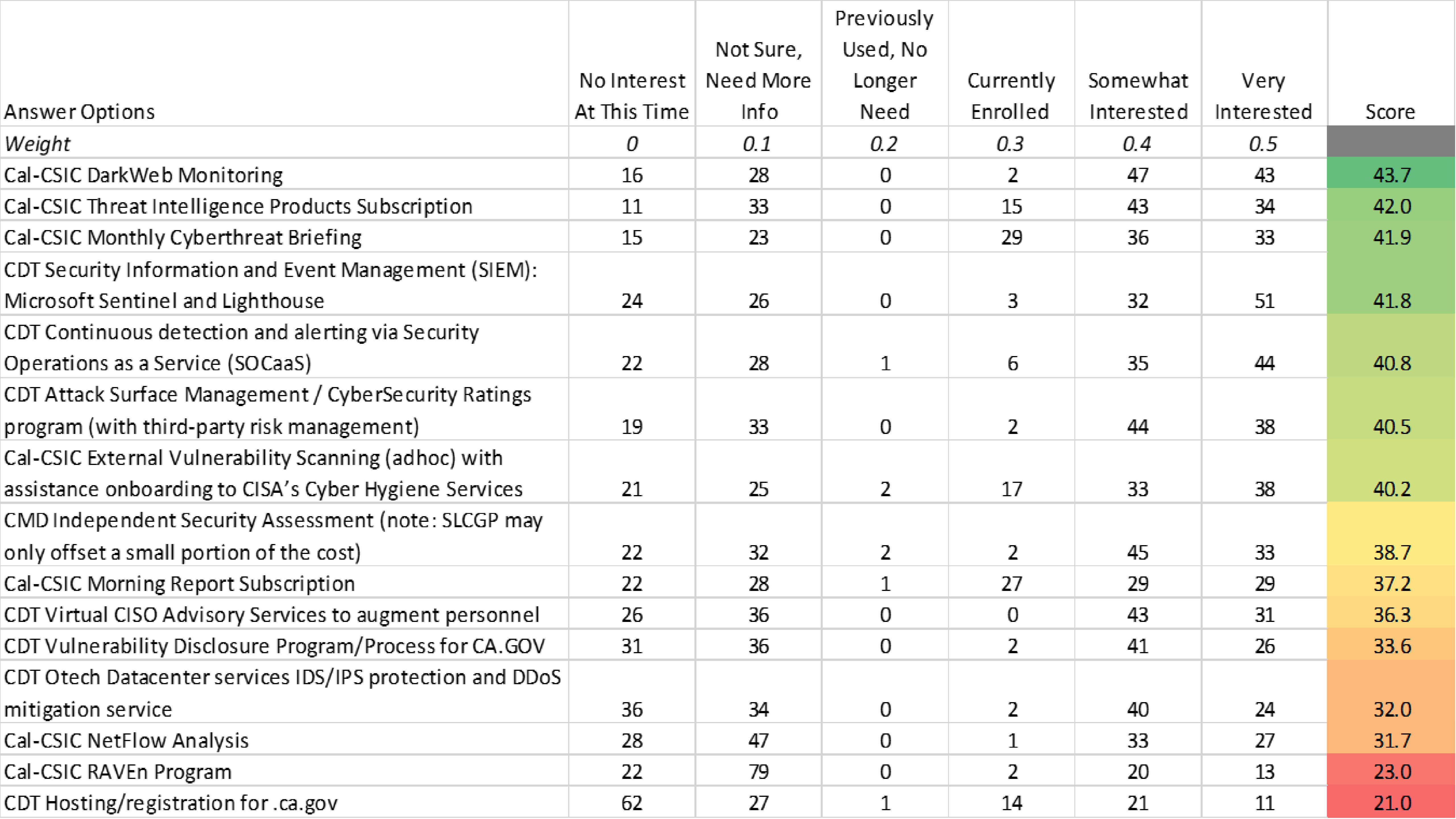
		1	2	3	4	5a	5b	5c	5d	5e	5f	5g	6	7	8	9	10	11	12	13	14	15	16	A	
Capability Level	Foundational	14	17	21	31	16	27	31	17	18	9	46	28	45	53	29	23	45	25	44	31	68	51	31	median = 33
Capability Level	Fundamental	52	50	54	45	34	46	44	49	35	34	31	39	42	45	45	50	42	39	49	49	20	19	42	average = 31.7
Capability Level	Intermediary	48	43	44	37	43	39	40	37	47	57	13	36	32	27	41	43	26	44	21	35	23	34	37	max = 68
Capability Level	Advanced	14	18	8	15	35	16	13	25	28	28	34	22	8	2	12	12	15	19	13	13	10	16	17	min = 2
Capability Gap	Planning	56	44	55	65	48	44	56	50	37	35	61	48	73	67	49	58	54	49	58	69	40	47	53	median = 45
Capability Gap	Organization	66	56	59	68	45	46	44	55	41	40	47	43	59	75	43	58	58	47	60	61	34	44	52	average = 44.4
Capability Gap	Equipment	55	64	45	47	39	72	52	51	34	44	17	20	31	24	44	42	28	14	27	26	21	19	37	max = 83
Capability Gap	Training	53	53	56	55	48	43	45	21	40	33	26	29	59	62	38	55	46	43	43	43	19	30	43	min = 14
Capability Gap	Exercises	51	46	63	44	22	24	28	15	25	53	17	24	83	43	49	52	40	25	35	39	17	19	37	
	Average	56	53	56	56	40	46	45	38	35	41	34	33	61	54	45	53	45	36	45	48	26	32		

				1	2	3	4	5a	5b	5c	5d	5e	5f	5g	6	7	8	9	10	11	12	13	14	15	16
	Survey Responses	Capability Level	Foundational	14	17	21	31	16	27	31	17	18	9	46	28	45	53	29	23	45	25	44	31	68	51
	By Element/Subelement	Capability Level	Fundamental	52	50	54	45	34	46	44	49	35	34	31	39	42	45	45	50	42	39	49	49	20	19
		Capability Level	Intermediary	48	43	44	37	43	39	40	37	47	57	13	36	32	27	41	43	26	44	21	35	23	34
		Capability Level	Advanced	14	18	8	15	35	16	13	25	28	28	34	22	8	2	12	12	15	19	13	13	10	16
			Average	32	32	32	32	32	32	32	32	32	32	31	31	32	32	32	32	32	32	32	32	30	30
		Capability Gap	Planning	56	44	55	65	48	44	56	50	37	35	61	48	73	67	49	58	54	49	58	69	40	47
		Capability Gap	Organization	66	56	59	68	45	46	44	55	41	40	47	43	59	75	43	58	58	47	60	61	34	44
		Capability Gap	Equipment	55	64	45	47	39	72	52	51	34	44	17	20	31	24	44	42	28	14	27	26	21	19
		Capability Gap	Training	53	53	56	55	48	43	45	21	40	33	26	29	59	62	38	55	46	43	43	43	19	30
		Capability Gap	Exercises	51	46	63	44	22	24	28	15	25	53	17	24	83	43	49	52	40	25	35	39	17	19
			Average	56	53	56	56	40	46	45	38	35	41	34	33	61	54	45	53	45	36	45	48	26	32
1	Manage, monitor, and track information systems, applications, and user accounts			↥																					
2	Monitor, audit, and track network traffic and activity				↥																				
3	Enhance the preparation/response/resiliency of InfoSys/apps/user accounts					↥																			
4	Continuous cybersecurity vulnerability assessments/threat mitigation prioritized by risk						↥																		
5a	Multi-Factor Authentication							↥																	
5b	Enhanced logging								↥																
5c	Data encryption for data at rest and in transit									↥															
5d	End use of unsupported/EOL software & hardware accessible from Internet										↥														
5e	Prohibit use of known/fixed/default passwords and credentials											↥													
5f	Ensure ability to reconstitute systems (backups)												↥												
5g	Migration to .gov internet domain													↥											
6	Promote delivery of safe/recognizable/trustworthy online services, including .gov														↥										
7	Ensure continuity of operations including by conducting exercises															↥									
8	Identify/mitigate workforce gaps, enhance recruitment/retention, bolster KSAs (NICE Framework)																↥								
9	Ensure continuity of comms & data networks																	↥							
10	Assess and mitigate, CIKR risks & threats impacting local jurisdictions																		↥						
11	Share cyber threat indicators with the State of California & DHS																			↥					
12	Leverage cybersecurity services offered by DHS (CISA)																				↥				
13	IT/OT modernization cybersecurity review process																					↥			
14	Develop and coordinate strategies to address cybersecurity risks & threats																						↥		
15	Ensure rural communities have adequate access to, and participation in plan activities																							↥	
16	Distribute funds, items, services, capabilities, or activities to local governments/agencies																								↥

CCTF CIPS Survey: Services vs. Cash

136 Responses





Answer Options	No Interest At This Time	Not Sure, Need More Info	Previously Used, No Longer Need	Currently Enrolled	Somewhat Interested	Very Interested	Score
Weight	*0*	*0.1*	*0.2*	*0.3*	*0.4*	*0.5*	
Cal-CSIC DarkWeb Monitoring	16	28	0	2	47	43	43.7
Cal-CSIC Threat Intelligence Products Subscription	11	33	0	15	43	34	42.0
Cal-CSIC Monthly Cyberthreat Briefing	15	23	0	29	36	33	41.9
CDT Security Information and Event Management (SIEM): Microsoft Sentinel and Lighthouse	24	26	0	3	32	51	41.8
CDT Continuous detection and alerting via Security Operations as a Service (SOCaaS)	22	28	1	6	35	44	40.8
CDT Attack Surface Management / CyberSecurity Ratings program (with third-party risk management)	19	33	0	2	44	38	40.5
Cal-CSIC External Vulnerability Scanning (adhoc) with assistance onboarding to CISA's Cyber Hygiene Services	21	25	2	17	33	38	40.2
CMD Independent Security Assessment (note: SLCGP may only offset a small portion of the cost)	22	32	2	2	45	33	38.7
Cal-CSIC Morning Report Subscription	22	28	1	27	29	29	37.2
CDT Virtual CISO Advisory Services to augment personnel	26	36	0	0	43	31	36.3
CDT Vulnerability Disclosure Program/Process for CA.GOV	31	36	0	2	41	26	33.6
CDT Otech Datacenter services IDS/IPS protection and DDoS mitigation service	36	34	0	2	40	24	32.0
Cal-CSIC NetFlow Analysis	28	47	0	1	33	27	31.7
Cal-CSIC RAVEn Program	22	79	0	2	20	13	23.0
CDT Hosting/registration for .ca.gov	62	27	1	14	21	11	21.0

		Gap Analysis Element Ranking																						
		Element	**1**	**2**	**3**	**4**	**5a**	**5b**	**5c**	**5d**	**5e**	**5f**	**5g**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	
Services	Services Survey Rank	Element Rank	12	16	1	2	8	17	13	9	11	22	19	20	6	4	18	5	15	21	14	3	7	10	Total Score
Cal-CSIC DarkWeb Monitoring	1			✓	✓	✓					✓			✓				✓	✓				✓	✓	87.0
Cal-CSIC Threat Intelligence Products Subscription	2				✓	✓								✓		✓		✓	✓	✓		✓	✓	✓	44.0
Cal-CSIC Monthly Cyberthreat Briefing	3				✓	✓								✓		✓		✓	✓	✓		✓	✓	✓	29.3
CDT Security Information and Event Management (SIEM): Microsoft Sentinel and Lighthouse	4		✓	✓	✓	✓		✓			✓			✓			✓	✓	✓				✓	✓	33.5
CDT Continuous detection and alerting via Security Operations as a Service (SOCaaS)	5		✓	✓	✓	✓		✓		✓	✓			✓	✓		✓	✓	✓				✓	✓	29.8
CDT Attack Surface Management / CyberSecurity Ratings program (with third-party risk management)	6		✓		✓	✓			✓	✓	✓			✓				✓					✓	✓	15.0
Cal-CSIC External Vulnerability Scanning (adhoc) with assistance onboarding to CISA's Cyber Hygiene Services	7				✓	✓				✓	✓			✓				✓		✓			✓	✓	12.3
CMD Independent Security Assessment	8				✓	✓				✓	✓			✓				✓				✓		✓	7.6
Cal-CSIC Morning Report Subscription	9				✓	✓								✓		✓		✓	✓	✓		✓	✓	✓	9.8
CDT Virtual CISO Advisory Services to augment personnel	10		✓		✓	✓			✓	✓	✓			✓	✓		✓	✓	✓				✓	✓	12.9
CDT Vulnerability Disclosure Program/Process for CA.GOV	11		✓		✓	✓		✓		✓	✓		✓	✓				✓	✓				✓	✓	11.6
CDT Otech Datacenter services IDS/IPS protection and DDoS mitigation service	12		✓	✓	✓	✓								✓	✓		✓	✓					✓	✓	8.1
Cal-CSIC NetFlow Analysis	13		✓	✓		✓								✓				✓					✓	✓	5.5
Cal-CSIC RAVEn Program	14					✓								✓				✓	✓				✓	✓	4.2
CDT Hosting/registration for .ca.gov	15		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓					✓	✓	12.5

Final Project Summary Worksheet (in Plan)

	Project Name	Project Description	Related Required Element #	Cost	Status	Priority	Project Type
1	DarkWeb Monitoring	State Government Service Option: Cal-CSIC DarkWeb Monitoring	2, 3, 4, 5e, 6, 10, 11, 15, 16	TBD	future	high	Equip
2	Threat Intelligence Subscription	State Government Service Option: Cal-CSIC Threat Intelligence Products Subscription, Monthly Cyberthreat Briefing, and Morning Reports	3, 4, 6, 8, 10, 11, 12, 14, 15, 16	TBD	future	high	Plan, Equip, Train
3	Security Information and Event Management (SIEM) Capability	State Government Service Option: CDT provisioned subscription to Microsoft Sentinel and Lighthouse	1, 2, 3, 4, 5b, 5e, 6, 9, 10, 11, 15, 16	TBD	future	high	Equip
4	Security Operations Center Capability	State Government Service Option: CDT Continuous detection and alerting via Security Operations as a Service (SOCaaS)	1, 2, 3, 4, 5b, 5d, 5e, 6, 7, 9, 10, 11, 15, 16	TBD	future	high	Organize, Equip
5	Virtual CISO Advisory Services	State Government Service Option: CDT Virtual CISO Advisory Services to augment personnel	1, 3, 4, 5a, 5b, 5c, 5d, 5e, 5f, 5g, 6, 9, 10, 11, 14, 15, 16	TBD	future	high	Plan, Organize, Train

California SLCGP Contacts & Resources

- For more information or to sign up:
  - California SLCGP website: **https://www.caloes.ca.gov/slcgp**
  - Please contact cctf-slcgp@caloes.ca.gov
- Clearly state your question and if you want to be added to the distro provide your:
  - First & last name (and go-by name if preferred)
  - Work email
  - Work phone
  - Organization and work title/position
  - State intent to be an active member or just want to receive informational updates
  - If not evident from your organization/position, please briefly describe your cybersecurity expertise/credentials if asking to join CCTF CIPS as an active member
  - ***Distro subscription is limited to government officials or representatives they specifically designate for SLCGP***
- Additional SLCGP Resources:
  - https://www.cisa.gov/state-and-local-cybersecurity-grant-program
  - https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program
  - FY22 NOFO: https://www.grants.gov/web/grants/view-opportunity.html?oppId=343579
  - FY23 NOFO: https://www.grants.gov/web/grants/view-opportunity.html?oppId=349776