State and Local Cybersecurity Grant Program (SLCGP)

Hawai‘i Office of Homeland Security

August 8, 2024

Table of Contents

1 Subrecipients

Eligible	Ineligible
• State, county government	• Nonprofit organizations
• State, county owned infrastructure	• Private corporations

2 Goal, Objectives, and Priorities

The implementation of the State and Local Cybersecurity Grant Program (SLCGP) in Hawai'i is guided by the Hawai'i Statewide Cybersecurity Strategy and Implementation Plan, published in September 26, 2023 that is a key enabler to establishing the Hawai'i Statewide Cybersecurity Program (HSCP). Included in that document are the overarching SLCGP requirements, including the mandated essential elements of the plan itself, as well as the projects the state plans to execute to improve its cybersecurity preparedness posture.

Nationally, the Department of Homeland Security state the goal of SLCGP is to assist state, local, and territorial governments with managing and reducing systemic cyber risk. For Fiscal Year 2022 (FY22), applicants are required to address how the following program objectives will be met in their applications. For FY23, applicants are required to address how the program objectives numbered two through four will be met in their applications.

- Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- Objective 3: Implement security protections commensurate with risk.
- Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

These broad outcomes are listed in logical sequence to aid recipients in focusing on the overall intent of the SLCGP and were adopted wholesale as the foundation of the HSCP. These outcomes will help establish prioritize the use of scarce resources and to develop metrics to gage success at both the project and organizational level. Outcomes of both the SLCGP and the HSCP will be measured by how well the state can improve the risk posture of the information systems they either own or those that are operated on their behalf.

2.1 Objective 1-Governance

- Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- Establish cybersecurity governance structures and implement a program to evaluate maturity of the cybersecurity program aligned to established by CISA and the National Institute of Standards Cybersecurity Performance Goals
- Participants have established and documented a uniform cybersecurity governance structure that is accountable to organizational leadership and works together to set the vision for cyber risk management.

- Participants have identified senior officials to enable whole-of-organization coordination on cybersecurity policies, processes, and procedures.
- Participants develop, implement, or revise, and test cybersecurity plans, including cyber incident response plans, with clearly defined roles and responsibilities.
- Participants develop, implement, or revise, and exercise cyber incident response plans e.g., participants conduct cyber tabletop exercises in accordance with industry best standards such as the NIST Cybersecurity Framework.
- Additional sub-objectives can be found in the official notice of funding (NOFO) document:
    - FEMA SLCGP NOFO 2022
    - FEMA SLCGP NOFO 2023

2.2 Objective 2-Assessment and Evaluation

- Participants should understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- Physical devices and systems, as well as software platforms and applications, are inventoried.
- Cybersecurity risk to the organization's operations and assets are understood.
    - Organization conducts an annual cyber risk assessment to identify cyber risk management gaps and areas for improvement
    - Organization annually completes the Nationwide Cybersecurity Review (NCSR).
    - Vulnerability scans are performed (internal scans), and a risk-based vulnerability management plan is developed and implemented.
        - Organization participates in **CISA's Vulnerability Scanning service**, part of the Cyber Hygiene program.
    - Organization effectively manages vulnerabilities by prioritizing mitigation of high impact vulnerabilities and those most likely to be exploited.
- Capabilities are in place to monitor assets to identify cybersecurity events.
    - Agencies are able to analyze network traffic and activity transiting or traveling to or from information systems, applications, and user accounts to understand baseline activity and identify potential threats.
        - The Multi-State Information Sharing and Analysis center offers the no-cost Malicious Domain Blocking and Reporting service to local units of government and publicly owned infrastructure.
- Processes are in place to action insights derived from deployed capabilities.
- Agencies are able to respond to identified events and incidents, document root cause, and share information with partners.
    - The Multi-State Information Sharing and Analysis Center (MS-ISAC) provides no-cost remote incident response capability to local units of government and publicly owned critical infrastructure.

2.3 Objective 3-Mitigation

- Implement security protections commensurate with risk. **RISK MUST BE UNDERSTOOD AND GOVERNANCE IN PLACE BEFORE OBJECTIVE 3 GRANTS CAN BE AWARDED.**
- Agencies adopt fundamental cybersecurity best practices.

- Implement multi-factor authentication (MFA), prioritizing privileged users, Internet- facing systems, and cloud accounts.
- End use of unsupported/end of life software and hardware that are accessible from the Internet.
- Prohibit use of known/fixed/default passwords and credentials.
- Ensure the ability to reconstitute systems following an incident with minimal disruption to services. (backups)
- Migrate to .gov or hawaii.gov internet domain.
- Individual participants address items identified through assessments and planning process in accordance with NIST CSF.
- Entities improve cybersecurity ecosystem by collaborating to address items identified through assessments and planning process (e.g., regional, and intra-state efforts)

2.4 Objective 4-Workforce Development

- Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility. **GOVERNANCE MUST BE IN PLACE BEFORE OBJECTIVE 4 GRANTS CAN BE AWARDED.**
- Personnel have the fundamental knowledge and skills necessary to recognize cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices.
- Regular ongoing phishing training, awareness campaigns are conducted, and organization provides role-based cybersecurity awareness training to all employees. Cybersecurity professionals attend technical training and conferences.

3 Funding

	FY 2022	%	FY 2023*	%	FY 2024*	%	FY 2025*	%
Federal Allocation	$2,243,539.00	100	$4,567,336.00	80	$3,362,000.00	70	$1,121,000.00	60
** State Match	Waived		$1,141,834.00	20	$1,440,857.14	30	$747,333.33	40
Total Available	$2,243,539.00	100	$5,709,170.00	100	$4,802,857.14	100	$1,868,333.33	100
Grant Administration	**$112,176.95**	**5**	**$280,187.50**	**5**	**$240,142.86**	**5**	**$93,416.67**	**5**
Objective 1: Governance and Planning	**$641,249.05**	**29**	**$570,917.00**	**10**	**$480,285.71**	**10**	**$373,666.67**	**20**
Statewide Cybersecurity Plan	$450,000.00	20					**$186,833.33**	**10**
Cyber Incident Response Plans	$100,000.00	14						
Cyber Incident Response Exercises	$91,249.05	4						
6. Threat Intelligence and Information Sharing			**$570,917.00**	**10**	**$480,285.71**	**10**	**$186,833.33**	**10**
Objective 2: Assessment and Evaluation	**$213,750.00**	**10**	**$1,427,292.50**	**25**	**$1,200,714.29**	**25**	**$280,250.00**	**15**
Develop asset protections and recovery actions.								
Continuous testing, education, evaluation, and structured assessments.								
Statewide inventory of devices, systems, software platforms, and applications.								
Foster understanding of organizational cybersecurity risks to operations and assets.								
Perform vulnerability scans; develop and implement a risk-based vulnerability management plan.								
Objective 3: Mitigation	**$848,863.00**	**38**	**$2,283,668.00**	**40**	**$1,921,142.86**	**40**	**$747,333.33**	**40**
5. Support Funding of Cybersecurity Projects at the County Level								
11. Develop Educational Materials on Cybersecurity Insurance								
3. Develop Purchasing Standards for 3rd-Party Vendors								
16. Secure and Enhance Connections in Cybersecurity Infrastructure								
Objective 4: Workforce Development	**$427,500.00**	**19**	**$1,141,834.00**	**20**	**$960,571.43**	**20**	**$373,666.67**	**20**
Workforce Development Strategy/Implementation Plans	$427,500.00	19						
2. Enhance Cybersecurity Workforce Recruitment and Staffing								
4. Develop and Deploy CRT Team								
10. Develop and Expand Relationships with Academic Partners								
14. Develop and Implement a Robust Cybersecurity Training Program								

3.1 Allowable Costs

For each grant year, the period of performance for purchases, contracts or other obligations may be funded for 48 months.

The 2023 SLCGP will fund a wide variety of cybersecurity projects, as articulated in the previously referenced Statewide Cybersecurity Strategy and Implementation Plan and detailed briefly above (with project reference numbers from that Implementation Plan, where applicable).

3.2 Unallowable Costs

The SLCGP funds may not be used for the following:

- Spyware;
- Construction and renovations involving modifications to existing buildings or structures that would require attaching equipment to walls, ceilings, floors, or doors including but not limited to:
    - Drilling new holes in walls, ceilings, or floors to install cable.
    - Installation of new conduit on to existing walls, ceilings, or floors.
    - Floor raising to install new cabling.
    - Installation of electrical outlets.
    - Any activities that involve ground disturbance.
- To pay a ransom;
- For recreational or social purposes;
- To pay for cybersecurity insurance premiums;
- For any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity that receives the grant;
- To supplant state or local funds; however, this shall not be construed to prohibit the use of funds from a grant under this NOFO for otherwise permissible uses on the basis that the recipient/subrecipient has previously used recipient/subrecipient funds to support the same or similar uses; and
- For any recipient or subrecipient cost-sharing contribution.

4 Grant Application Process

4.1 Step 1 – Gap Assessment

- Applicants should complete the online cybersecurity gap assessment found on the online grant portal – CLICK HERE to open the Gap Assessment
- The gap assessment will help applicants determine which objectives to prioritize within their respective application. Note: the gap assessment is *NOT* a cybersecurity vulnerability assessment and does not count toward that objective.
- Upon completion of the gap assessment the applicant will receive an automated email with additional information/instructions and should continue to step two – self certification (if required) or continue to step three if a self-certification is not required.

4.2 Step 2 – Self Certification

- Not every application to the SLCGP requires self-certification. Only applicants that meet the following criteria are required to submit a self-certification document(s).
    - Entities with cybersecurity governance in place. Cybersecurity governance is considered IT or cybersecurity personnel (this includes in-house IT or cybersecurity personnel as well as contracted 3rd parties that handle either or both responsibilities).
    - Entities that have completed cybersecurity vulnerability assessments within 12 months of signing the self-certification document. (These assessments may be completed by in-house personnel or may be completed by 3rd party private contractors, CISA, DHS, or other entities)
- *Only applicants who submit the appropriate self-certification are eligible to apply for equipment/services that meet objectives 2 or 3.*
- The self-certification documents can be found on the OHS SLCGP grant portal – CLICK HERE to view the webpage.
- Note: The only *exception* to the required self-certifications will be applications for the emergency replacement of public/externally facing legacy (outdated and unsupported) equipment/software. But the applicant should be wary of the fact that new equipment will quickly become vulnerable to cyber-attacks if there are no personnel, policies, or guidelines in place to protect it. Furthermore, it should be a priority of the applicant to secure those resources (personnel, polices, guidelines) as quickly as possible and the applicant will be required to provide a plan within their application to outline a course of action to do so.

4.3 Step 3 – Grant Application

- The SLCGP application should not be completed until the Gap Assessment from step one has been completed – reference Step 1 above.
- The Grant Application documents (Project Narrative and Budget Table) can be found on the OHS SLCGP grant portal – CLICK HERE to view the webpage.

4.3.1 General Procedures

- **Quote** – Applicants should obtain a quote from equipment or service vendor(s) (a single quote is required)
- **Grant Award ID** – Applicants will need to include a grant Award ID with every

application. The Grant Award ID is provided by OHS via email upon completion of the Gap Assessment.

- **UEI** - *Effective April 4, 2022*, the Federal Government transitioned from using the Data Universal Numbering System or *DUNS number*, to a new, non-proprietary identifier known as a **Unique Entity Identifier** or UEI. For entities that had an active registration in the System for Award Management (SAM.gov) prior to this the UEI has automatically been assigned and no action is necessary. For all entities filing a new registration in SAM.gov on or after April 4, 2022, the UEI will be assigned to that entity as part of the SAM.gov registration process.
    - UEI registration information is available on GSA.gov at: Unique Entity Identifier Update | GSA. Grants.gov registration information can be found at: https://www.grants.gov/web/grants/register.html
- **SAM.gov** – All applicants should be registered on sam.gov - https://www.sam.gov/SAM/
    - The SAM quick start guide for new recipient registration and SAM video tutorial for new applicants are tools created by the General Services Administration (GSA) to assist those registering with SAM. If applicants have questions or concerns about a SAM registration, please contact the Federal Support Desk at https://www.fsd.gov/fsd-gov/home.door or call toll free (866) 606-8220.
- **EIN** - All entities applying for funding must provide an Employer Identification Number (EIN). The EIN can be obtained from the IRS by visiting: https://www.irs.gov/businesses/small-businesses- self-employed/apply-for-an-employer-identification-number-ein-online (instructions on *page 21 of the NOFO*)
- **Procurement Guidelines** - Applicants must agree to follow Hawai'i Public Procurement Code, Hawai'i Revised Statutes Chapter §103D.
- **Authorized Equipment** - Unless otherwise stated, all equipment purchases must meet all applicable statutory, regulatory, and DHS standards to be eligible for purchase using these funds. Please refer to FEMA's Authorized Equipment List | FEMA.gov. In addition, recipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment.
- **Emergency Communications** - Investments in emergency communications systems and equipment must meet applicable SAFECOM Guidance recommendations. Such investments must be coordinated with the Statewide Inoperability Coordinator (SWIC) and the State Interoperability Governing Body (SIGB) to ensure interoperability and long-term compatibility.

4.3.2 Definitions

- **Project Category** (Appendix D of FEMA SLCGP NOFO 2023) – Approved categories include:
    - **Planning** – Planning costs are allowable under this program. SLCGP funds may be used for a range of planning activities, such as those associated with the development, review, and revision of the holistic, entity-wide Cybersecurity Plan and other planning activities that support the program goals and objectives.
    - **Organization** – Organization costs are allowable under this program. States must justify proposed expenditures of SLCGP funds to support organization activities

within their Investment Justification submission. Organizational activities include:

- Program management;
- Development of whole community partnerships that support the Statewide Cybersecurity Program;
- Structures and mechanisms for information sharing between the public and private sector; and
- Operational support.
- Personnel hiring, overtime, and backfill expenses are permitted under this grant to perform allowable SLCGP planning, organization, training, exercise, and equipment activities. Personnel expenses may include, but are not limited to training and exercise coordinators, program managers and planners, and cybersecurity navigators.

- **Exercises** - Exercise costs are allowable under this program. Exercises conducted with grant funding should be managed and conducted consistent with Homeland Security Exercise and Evaluation Program (HSEEP). Additionally, applicants are encouraged to utilize existing no-cost CISA resources whenever possible. A complete list of CISA tabletop packages can be found here.
- **Training** – May be supported if it aligns with grant objectives 1-3 and the applicant completes the appropriate self-certification documents. Recipients are also encouraged to coordinate in-state sponsorship of available cybersecurity training offerings from FEMA's National Preparedness Course Catalog and the National Cybersecurity Preparedness Consortium with the Hawai'i Office of Homeland Security Planning and Operations Branch.
- **Equipment** - Unless otherwise stated, all equipment must meet all applicable statutory, regulatory, and DHS standards to be eligible for purchase using these funds. Please refer to FEMA's Authorized Equipment List | FEMA.gov. In addition, recipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment.

- **Project Name** – Provided by applicant. Give the project a descriptive title.
- **Project Purpose** – A one sentence summary of the project.
  - **Required Elements** – There are 16 required elements, and most projects will address more than one of them. Chose all required elements that your project will address.
    - Manage, monitor, and track information systems, applications, and user accounts
    - Monitor, audit, and track network traffic and activity
    - Enhance the preparation, response, and resilience of information systems, applications, and user accounts
    - Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by risk
    - Adopt and use best practices and methodologies to enhance cybersecurity
      - Implementation of multi-factor authentication.

        - End the use of unsupported/end of life software and hardware that are accessible from the Internet.
        - Prohibition against use of known/fixed/default passwords and credentials.
        - Ensure the ability to reconstitute systems (backups); and
        - Migration to the .gov internet domain.
        - Implement enhanced logging.
        - Data encryption for data at rest and in transit.
    - Promote the delivery of safe, recognizable, and trustworthy online services, including through the use of the .gov internet domain
    - Ensure continuity of operations including by conducting exercises
    - Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)
    - Ensure continuity of communications and data networks in the event of an incident involving communications or data networks
    - Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems
    - Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department
    - Leverage cybersecurity services offered by the Department
    - Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives
    - Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats
    - Ensure rural communities have adequate access to, and participation in plan activities
    - Distribute funds, items, services, capabilities, or activities to local entities
- **Project Status – future, ongoing, or complete**

4.3.3 Funding

- Funding Request = Estimated cost of project-20% cost share match.
- Formula for Calculating Cost Share for Projects - please see the following example: Formula: Total Project Cost x Cost Share Percentage of the Project = Cost Share Amount; Total Project Cost x Federal Percentage Share of the Project = Federal Amount for the Project
    - Example: If the total project cost is $125,000, the cost share percentage of the project is 20% and the federal percentage share of the project is 80%, the cost share amount for the project and federal amount for the project is calculated

below:

- $125,000 x .20 = $25,000 (Cost Share Amount for Project)
- $125,000 x .80 = $100,000 (Federal Share Amount for Project)

- **Cost Share Match Waiver** – Applicants who apply for a cost share waiver must be able to demonstrate economic hardship. **Additional details can be found in the appropriate NOFO funds are being requested from**. For local units of government, demonstration that those localities have areas within them that are designated as either "high" or "very high" on the Centers for Disease Control and Prevention's Social Vulnerability Index are eligible to have cost share waived.

4.3.4 Narrative Examples

- **Project**

Since [year], [Organization Name] has provided [this critical service/core capability] to [area name, list or count of cities, counties and/or regions served, approximate total population served]. Our organization has [approximate number of employees] and [number] devices on our network. Our core capability(s) mentioned above, rely on our IT infrastructure [why is your IT or Operational Technology integral to performing your key operational functions?]. [Organization Name] is applying for this SLCGP funding to [manage THIS risk. (if you know what your risks are, if not you should be applying to determine your risk), What is the grant for specifically (what equipment/services)? Why do you want to do this? How will it protect your critical assets and the communities/organizations that rely on you?]. [what have you already done to improve your organizations cybersecurity? e.g., training, hired people to manage your environment, used CISA resources, joined MS-ISAC or other ISAC, had consultations, etc.] Why is this the next logical step or is it the first step?

- **Investment Strategy**

[*Describe in narrative form how your project strategy effectively demonstrates the objectives of preventing, preparing for, protecting against, and responding to cyber incidents. Proposals must address closing the gaps in applicants' identified core capabilities and reducing the overall risk to the community, state or nation. (Refer to the four program objectives and 16 required elements as well as your responses in the gap assessment and any cyber vulnerability or risk assessments performed in the last 12 months.)]*

- **Collaboration**

[*Regional, statewide or multi-state impact. Describe in narrative form the extent to which the project demonstrates a willingness to collaborate with federal, state, and local governments in efforts to prevent, prepare for, protect against, and respond to acts of cyber-crime and reduce the overall risk to the state or the nation. (also include consultations with similar agencies, city, county, regional, state, federal or private 3rd party entities as well as any DHS, MS-ISAC or CISA services leveraged by your organization to include: Memberships, Training, Exercises, Information Sharing, Incident Response etc.)*]

- **Budget**

[Quote, budget table, budget narrative, funding request and match should all sync up. Describe

in narrative form your project's budget plan, demonstrating how it will maximize cost effectiveness of grant expenditures. What is the plan for financial sustainability (how will you maintain the respective services/equipment after the life of the grant)? Are local matching funds available? Will you be doing an in-kind match? Will you be submitting a match waiver?]

4.3.5 Sustainability Timeline

	2022	2023	2024	2025	After Grant
SLCGP	Business impact analysis, cyber policies, replace legacy systems	MSP	MFA, Backups, .gov, MSP	Train Personnel (CompTIA, SANs certifications), MSP	MSP, track legacy systems, train personnel
Objectives	1,2	2	3	4	
Required Elements	1, 5, 11, 12, 14	2, 5, 7, 11, 12	3, 5, 6, 11, 12	8, 12	12

4.3.6 Attachments

Unless otherwise indicated, the following documents should be attached to your completed application.

- Completed (and signed) copy of cyber governance self-certification.
- Completed (and signed) copy of cyber vulnerability/risk assessment self-certification.
- Budget.xls file (should match your budget narrative exactly)
- City/County resolution
- Print out of Authorized Equipment List (AEL) Documentation
- Print out from SAM.gov showing active entity registration
- One (1) price quote for requested equipment
- Labeled photos if project requires equipment installation to the inside or outside of a building, tower or any other structure
- Project Narrative
- Others as identified within the application

5 The SLCGP Grant Review and Award Process

5.1 Peer Review Panel

The Hawai‘i State and Local Cybersecurity Grant Program (SLCGP) chartered Working Group (SLCGP Working Group) will select a peer review panel consisting solely of its members. The panel may have as few as four members but with no defined maximum to assess the feasibility and efficacy of each subrecipient project and respective proposal. Peer review panel members will then read and sign a SLCGP conflict of interest form prior to beginning the review process. Panel members are prohibited from scoring any grant that qualifies as such a conflict. To further minimize conflict of interest, grant peer review panelists will only review applications from outside their jurisdiction.

Individual grants will be assessed and given a score from 0-100 based on the following criteria:

- Investment Strategy
- Collaboration with state or county entities
- Budget Narrative
    - Cost Effectiveness
    - Financial Sustainability
- Project Impact/Outcomes
    - Procedures implemented and capabilities enhanced
    - Threats and hazards mitigated
    - Improvement/progress measurement/evaluation
- How well does this project align with SLCGP priorities outlined in the Hawai‘i Statewide Cybersecurity Strategy and Implementation Plan and the current year’s NOFO

Each grant must be reviewed by two or more peer review panel members and will receive two or more scores.

Scores for each individual application will then be averaged to establish a ranked list of all subrecipient project proposals.

5.2 Final Project Selection

The SLCGP Working Group (requires a quorum of members) will convene and use application scores to identify projects that best adhere to grant funding priorities and allocate projects into categories of fully funded, partially funded, or not funded.

If the total award amount applied to the funding proposals for categories of “fully funded” and “partially funded” exceeds SLCGP funds available, the SLCGP Working Group will decide which project awards to modify, in keeping with priorities from the Hawai‘i Statewide Cybersecurity Strategy and Implementation Plan and the current year’s NOFO.

Alternatively, if the sum of the funding proposals for categories of “fully funded” and “partially funded” do not equal or exceed the SLCGP funds available, the SLCGP Working Group will decide which projects to modify, in keeping with priorities from the Hawai‘i Statewide Cybersecurity Strategy and Implementation Plan and the current year’s NOFO.

6 After the Application/Upon Award

Award letters are e-mailed to the local subrecipients within 45 calendar days of the SAA receipt of SLCGP funds. The award letter serves as supporting documentation that the SAA has met the 80% passthrough funding requirement to the local units of government.

Sub-recipients must sign up for cyber hygiene services, specifically vulnerability scanning and web application scanning.

Sub-recipients must Complete the Nationwide Cybersecurity Review, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually thereafter.

MS-ISAC members are encouraged to sign up for Malicious Domain Blocking and Reporting (MDBR).

All Sub-Recipient staff, including Authorizing Officials, Project Directors, and Financial Directors, must schedule and attend grant agreement meeting with the OHS grant staff. The grant agreement meetings emphasize compliance and provide detailed instructions on all policy and procedures, including procurement methods, prior to executing the grant agreement.

6.1 State Authorized Agency Procedures Upon Award

- **Federal Funding Accountability and Transparency Act of 2006 (FFATA)**

The Hawai‘i Office of Homeland Security Grants Management Branch enters and submits necessary data into the Federal Funding Accountability and Transparency Act of 2006 (FFATA) required report. This database includes all state and local sub- recipients; amount of award; funding agency; Catalog of Federal Domestic Assistance (CFDA) program number; award title; location of the entity and primary location of performance including city, state, and Congressional district; and, the Unique Entity ID (UEI #). This information is supplied for all sub-recipients receiving $30,000 or more in federal funds.

- **Sub-Recipient Grant Agreements**

Scopes of Work for each agreement are reviewed and approved by the Hawai‘i Office of Homeland Security Grants Management Branch.

Grant agreements are created for each individual sub-recipient. Each Grant Agreement will be routed via esign by the sub-recipient Authorizing Official, the OHS Administrator, and State Deputy Attorney General. The Grant Agreement will also include the grant award notice and project information.

- **Sub-Recipient Grant Project Files**

A file folder is created for each grant project. The grant project folder is labeled by the lead applicants name and the application project number. The file folder contains the following information:

- Original grant application.
- Award letter to sub-recipient.
- Fully Executed Grant Agreement and any modifications.

- Budget Information
- Procurement Policy
- Validation of authorized legal signatures for sub-recipient.
- Ledger identifying each payment, year to date expenditures, and available balance.
- Validation of current SAM.GOV registration.
- Proof of NCSR Survey.
- Proof of cyber hygiene services.
- Single Audit status verification.
- Quarterly Reports
- Correspondence in chronological order – Emails, Telephone calls documented by a memo to the file
- Close-out monitoring report and official close-out letter.

- **Sub-Recipient Grant Reimbursement Process**

To request for reimbursements, the subrecipient will provide documentation, to include a copy of the contract or purchase order documents that identifies equipment, or services requested with a Transmittal Reimbursement Form to OHS within 15 days of the expenditure.

The sub recipient will need to submit the reimbursement request via email to OHS for review. Once everything is approved, the sub recipient will only need to mail the original signed transmittal reimbursement form to OHS.

OHS will prepare a purchase order for the reimbursement request. OHS will route the purchase order for esignatures to the Grants Manager and OHS Administrator. The purchase order will be routed to the financial department to assign a purchase order number. Thereafter, the financial department will drawdown the funds under the grant, which initiates the following activities:

- The State Budget and Finance will cut a check and mail the check to OHS for processing.
- OHS will mail the check via certified mail to the sub recipient.
- OHS will verify when the check has been cashed via cash warrants.
- Reimbursement takes approximately 4-6 weeks for processing.

6.1.1 Sub Recipient Quarterly Reporting

OHS will send out a Quarterly Expenditure and Tracking Workbook for the subrecipient to complete. The subrecipient is obligated to complete and submit the quarterly reports to OHS by the 5th day of the month following the end of each quarter.

The Quarterly Expenditure and Tracking Workbook provides compliance with the DHS/FEMA reporting requirement. The workbook will provide investments and projects based on the budget related to encumbrances and expending the allocated funds. Providing updates over a 90-day period is important to assess the progress of the projects. This information from this report will feed into DHS/FEMA performance progress Reports that OHS completes on a semiannual basis (June 30th and December 31st).

6.1.2 Sub-Recipient Desk Review and Site Monitoring Visit

A site visit is scheduled with the project manager and any staff they deem necessary. The subrecipient project grant files are reviewed for completeness, accuracy, and state or federal

audit compliance.

6.1.3 Closeout Procedures

A close out report is completed by the Grant Manager verifying that documents, scope of work, and financial activity are accurate and complete. An official closeout letter is created, signed by the OHS Executive Director, and sent to the sub- recipient's Authorized Official, Project Manager, and Financial Officer.