DEPARTMENT OF DEFENSE

RELEASE DATE: March 3, 2023

REQUEST FOR PROPOSALS
Job No. RFP-CA-202212

SEALED OFFERS
FOR

Plan Development and Supporting Activities

STATE OF HAWAI'I
DEPARTMENT OF DEFENSE
OFFICE OF HOMELAND SECURITY

WILL BE RECEIVED UP TO 2:00 P.M., (HST) ON

APRIL 5, 2023

IN THE STATE OF HAWAI'I, DEPARTMENT OF DEFENSE, ENGINEERING OFFICE, BUILDING 306A, ROOM 228, 3949 DIAMOND HEAD ROAD, HONOLULU, HAWAI'I 96816.

DIRECT QUESTIONS RELATING TO THIS SOLICITATION TO STATE OF HAWAI'I, DEPARTMENT OF DEFENSE, ENGINEERING OFFICE, MS. THEASIUS ALLEN, TELEPHONE (808) 369-3483, OR BY E-MAIL AT THEASIUS.A.ALLEN@HAWAII.GOV

Major General, KENNETH S. HARA
Hawai'i National Guard
Adjutant General

TABLE OF CONTENTS

SECTION ONE

INTRODUCTION, TERMS AND ACRONYMS, KEY DATES

1.1 INTRODUCTION

The State Department of Defense (DOD), Office of Homeland Security (OHS) is requesting proposals from a qualified contractor to plan, facilitate, and write a Plan development for a series of strategies, implementation and response plans and their supporting exercises related to **Targeted Violence Prevention**, **Critical Infrastructure Security and Resilience**, and **Cybersecurity**. Any award will result in a contract for the PLAN DEVELOPMENT AND SUPPORTING ACTIVITIES, for the use by the State DOD-OHS.

1.2 CANCELLATION

The Request for Proposals (RFP) may be cancelled and any or all proposals rejected in whole or in part, without liability to the State, when it is determined to be in the best interest of the State.

1.3 TERMS AND ACRONYMS USED THROUGHOUT THE SOLICITATION

BAFO	=	Best and Final Offer
CPO	=	Chief Procurement Officer
DAGS	=	Department of Accounting and General Services
DOD	=	Department of Defense
GC	=	General Conditions, issued by the Department of the Attorney General
GET	=	General Excise Tax
GP	=	General Provisions
HAR	=	Hawai'i Administrative Rules
HRS	=	Hawai'i Revised Statutes
OHS	=	Office of Homeland Security
Procurement Officer	=	The contracting officer for the State of Hawai'i, State Procurement Office
RFP	=	Request for Proposals
State	=	State of Hawai'i, including its departments, agencies, and political subdivisions

1.4 RFP SCHEDULE AND SIGNIFICANT DATES

The schedule represents the State's best estimate of the schedule that will be followed. All times indicated are Hawai'i Standard Time (HST). If a component of this schedule, such as "Proposal Due date/time" is delayed, the rest of the schedule will likely be shifted by the same number of days. Any change to the RFP Schedule and Significant Dates shall be reflected in and issued in an addendum. The approximate schedule is as follows:

Release of Request for Proposals	March 3, 2023
Pre-proposal Conference via Microsoft TEAMS	March 8, 2023 / 10:30 A.M.
Due date to Submit Questions	March 15, 2023 / 4:30 P.M.
State's Response to Questions	March 20, 2023
Proposals Due date/time	April 5, 2023 / 2:00 P.M.
Proposal Evaluations	April 5, 2023
Discussion with Priority Listed Offerors (if necessary)	April 11, 2023
Best and Final Offer (if necessary)	April 11, 2023
Estimated Notice of Award	April 14, 2023
Estimated Contract Start Date	May 1, 2023

1.5 PRE-PROPOSAL CONFERENCE

The purpose of the pre-proposal conference is to provide Offerors an opportunity to be briefed on this procurement and to ask any questions about this procurement. The pre-proposal conference is not mandatory; however, Offerors are encouraged to attend to gain a better understanding of the requirements of this RFP.

Offerors are advised that anything discussed at the pre-proposal conference does not change any part of this RFP. All changes and/or clarifications to this RFP shall be done in the form of an addendum.

Submit your email address to theasius.a.allen@hawaii.gov by 2:00 P.M., before March 7, 2023. All participants will be sent a Microsoft TEAMS meeting invite.

The pre-proposal conference will be held as follows:

Date: March 8, 2023

Time: 10:30 A.M. – until session is complete

Location: Via Microsoft TEAMS

1.6 QUESTIONS AND ANSWERS PRIOR TO OPENING OF PROPOSALS

All questions must be submitted in writing to the Engineering Office, Contract Assistant Theasius Allen via e-mail at theasius.a.allen@hawaii.gov by the due date specified in Section 1.4, *RFP Schedule and Significant Dates,* as amended.

The State will respond to questions through Addenda/Amendments by the date specified in Section 1.4, *RFP Schedule and Significant Dates,* as amended.

SECTION TWO

BACKGROUND AND SCOPE OF WORK

2.1 PROJECT OVERVIEW AND HISTORY

The Office of Homeland Security (OHS), currently situated within the State DOD, is tasked to assist State, federal and local partners, and law enforcement authorities in providing for the safety, welfare, and defense for the people of Hawai'i. No single agency at the local, state, federal, or private level possesses the authority and the expertise to act unilaterally on the many complex issues that could arise in response to Homeland Security threats. Action requires open communication and coordination between and among OHS and various public and private partners, especially law enforcement, public safety, public health, and emergency management.

Development and implementation of these plans and its activities through a collaborative effort among the federal, State, and county governments, and the private sector enhances our Homeland Security posture.

2.2 SCOPE OF WORK

All services and for who services are to be provided for shall be in accordance with this RFP, including its attachments and any addenda.

The State of Hawai'i DOD-OHS is seeking consulting services to assist in the development of a series of strategies, implementation and response plans and activities their supporting exercises related to **Targeted Violence Prevention**, **Critical Infrastructure Security** and **Resilience, and Cybersecurity**. The OHS requests that one of the planning methodologies used in the plan will be response techniques, processes by employing the response community, stakeholders, subject matter experts and others to support identification of capabilities, resources, and gaps.

1. Project Goal and Objectives/Milestones

A. Project Goal

The goal of this project is to develop a series of strategies and response plans and their supporting exercises related to the objectives below:

B. Objectives

1. **Develop Targeted Violence Prevention Strategy Implementation Plan**: Utilizing the Hawai'i Targeted Violence Prevention Strategy (Attachment Exhibit D1) and related reference materials, as well as stakeholder outreach and engagement, develop a three (3) year Implementation Plan that includes: the 11 identified goals from the strategy and their related Objectives, Tasks, Outputs, Outcomes, and Measures of Implementation, as well as Lead Stakeholder Implementor.

2. **Develop Critical Infrastructure Security & Resilience Strategy Implementation Plan**: Utilizing the Department of Homeland Security's Infrastructure Resilience Planning Framework (Attachment Exhibit D2), the Hawai'i Critical Infrastructure

Security & Resilience Strategy, related reference materials, and informed by relevant ongoing activities; develop and execute an Implementation Plan for establishing a critical infrastructure data management system. The Implementation Plan will articulate the conduct of a comprehensive inventory and baseline interdependency assessment of the state's critical infrastructure and their dependencies/interdependencies to inform the development of threat mitigation activities, incident response capabilities and capacity, and long-term resiliency investment planning. The plan and its execution will be informed by and synchronized to current critical infrastructure inventories and related data and the system(s) they are contained in. The ultimate purpose of this project is to collect and document data and information that portrays the critical infrastructure ecosystem in Hawai'i to better characterize vulnerability and risk in order to inform resource prioritization of resilience activities.

3. **Develop a Statewide Cybersecurity Strategy and Implementation Plan(s):** Utilizing the guidelines outlined in the **2022 State and Local Cybersecurity Grant Program** (SLCGP) (Attachment Exhibit D4) Notice of Funding Opportunity and related reference materials, as well as stakeholder outreach and engagement through the Hawai'i SLCGP Subcommittee, develop a statewide multi-year strategy and supporting Implementation Plan(s) – at both the subrecipient and state levels.

4. **Develop Subrecipient Cyber Incident Response Plans**: Develop subrecipient (of the SLCGP) Cyber Incident Response Plans, synchronized to state Cyber Disruption Response Plan (Attachment Exhibit D3) and modeled after the Office of Enterprise Technology Services Cyber Incident Response Plan; as each are completed, develop and implement field county/entity Cyber Incident Response Plan Exercises.

5. **Develop Statewide Cyber Workforce Development Strategy and County/Entity-Level Implementation Plans**: Utilizing the guidelines outlined in the **2022 State and Local Cybersecurity Grant Program** (SLCGP) (Attachment Exhibit D4) Notice of Funding Opportunity and related reference materials, as well as stakeholder outreach and engagement through the Hawai'i SLCGP Subcommittee, develop Statewide Cyber Workforce Development Strategy and County/Entity-Level Implementation Plans, to include a continuous testing, evaluation, and structured assessments approach, as well as data gathering schema and metrics.

2.3 CONTRACT TYPE

Any contract award resulting from this solicitation will be a firm-fixed price contract payable upon successful completion of performance milestones.

2.4 TERM OF CONTRACT

The contract shall be for a period of 24 months from the date of the Notice to Proceed and is intended to begin approximately May 2023 and end on April 30, 2025.

Unless terminated, the Contractor and the State may extend the term of the contract for up to four (4) additional 12-month periods or portions thereof without the necessity of re-soliciting, upon mutual agreement in writing at least sixty (60) days prior to the expiration of the contract. The contract price or commission paid to the Contractor for the extended period shall remain the same or as described in the offer.

When interests of the State or the Contractor so require, the State or the Contractor may terminate the contract for convenience by providing six (6) weeks prior written notice to the other party.

2.5 CONTRACT ADMINISTRATOR

For the purposes of this contract, Frank Pace, Homeland Security Administrator, (808) 369-3570, or authorized representative, is designated the Contract Administrator.

SECTION THREE

PROPOSAL FORMAT AND CONTENT

3.1 OFFEROR'S AUTHORITY TO SUBMIT AN OFFER

The Office of Homeland Security (OHS) a division within the State of Hawai'i Department of Defense (DOD) will not participate in determinations regarding an Offeror's authority to sell a product or service. If there is a question or doubt regarding an Offeror's right or ability to obtain and sell a product or service, the Offeror shall resolve that question prior to submitting an offer by the due date specified in Section 1.4, *RFP Schedule and Significant Dates,* as amended.

3.2 REQUIRED REVIEW

3.2.1 Before submitting a proposal, each Offeror must thoroughly and carefully examine this RFP, any attachment, addendum, and other relevant document, to ensure Offeror understands the requirements of the RFP. Offeror must also become familiar with State, local, and Federal laws, statutes, ordinances, rules, and regulations that may in any manner affect cost, progress, or performance of the work required.

3.2.2 Should Offeror find defects and questionable or objectionable items in the RFP, Offeror shall notify the Department of Defense, Engineering Office in writing to the Engineering office Contract Assistant, Theasius Allen via e-mail at theasius.a.allen@hawaii.gov prior to the deadline for written questions as stated in the RFP *Schedule and Significant Dates*, as amended. This will allow the issuance of any necessary corrections and/or amendments to the RFP by addendum and mitigate reliance of a defective solicitation and exposure of proposal(s) upon which award could not be made.

3.3 PROPOSAL PREPARATION COSTS

Any and all costs incurred by the Offeror in preparing or submitting a proposal shall be the Offeror's sole responsibility whether or not any award results from this RFP. The State shall not reimburse such costs.

3.4 TAX LIABILITY

3.4.1 Work to be performed under this solicitation is a business activity taxable under HRS Chapter 237, and if applicable, taxable under HRS Chapter 238. Contractor is advised that they are liable for the Hawai'i GET at the current 4.712% for sales made on Oahu, and at the rate for the islands of Hawai'i 4.4386%, Maui 4.1666%, and Kauai 4.712%. If, however, an Offeror is a person exempt by the HRS from paying the GET and therefore not liable for the taxes on this solicitation, Offeror shall state its tax exempt status and cite the HRS chapter or section allowing the exemption.

3.4.2 Federal I.D. Number and Hawai'i General Excise Tax License I.D. Offeror shall submit its current Federal I.D. No. and Hawai'i General Excise Tax License I.D. number in the space provided on Offer Form, page OF-1, thereby attesting that the Offeror is doing business in the State and that Offeror will pay such taxes on all sales made to the State.

3.5 PROPERTY OF STATE

All proposals become the property of the State of Hawai'i.

3.6 CONFIDENTIAL INFORMATION

3.6.1 If an Offeror believes that any portion of a proposal, offer, specification, protest, or correspondence contains information that should be withheld from disclosure as confidential, then the Offeror shall inform the Procurement Officer named on the cover of this RFP in writing and provided with justification to support the Offeror's confidentiality claim. Price is not considered confidential and will not be withheld.

3.6.2 An Offeror shall request in writing nondisclosure of information such as designated trade secrets or other proprietary data Offeror considers to be confidential. Such requests for nondisclosure shall accompany the proposal, be clearly marked, and shall be readily separable from the proposal in order to facilitate eventual public inspection of the non-confidential portion of the proposal.

3.7 EXCEPTIONS

Should Offeror take any exception to the terms, conditions, specifications, or other requirements listed in the RFP, Offeror shall list such exceptions in this section of the Offeror's proposal. Offeror shall reference the RFP section where exception is taken, a description of the exception taken, and the proposed alternative, if any. The State reserves the right to accept or not accept any exceptions.

No exceptions to statutory requirements of the AG General Conditions shall be considered.

3.8 PROPOSAL OBJECTIVES

3.8.1 One of the objectives of this RFP is to make proposal preparation easy and efficient, while giving Offerors ample opportunity to highlight their proposals. The evaluation process must also be manageable and effective.

3.8.2 Proposals shall be prepared in a straightforward and concise manner, in a format that is reasonably consistent and appropriate for the purpose. Emphasis will be on completeness and clarity and content.

3.8.3 When an Offeror submits a proposal, it shall be considered a complete plan for accomplishing the tasks described in this RFP and any supplemental tasks the Offeror has identified as necessary to successfully complete the obligations outlined in this RFP.

3.8.4 The proposal shall describe in detail the Offeror's ability and availability of services to meet the goals and objectives of this RFP as stated in Section 2.2 SCOPE OF WORK.

3.8.5 Offeror shall submit a proposal that includes an overall strategy, timeline and plan for the work proposed as well as expected results and possible shortfalls.

3.9 PROPOSAL FORMS

3.9.1 To be considered responsive, the Offeror's proposal shall respond to and include all items specified in this RFP and any subsequent addendum. Any proposal offering any other set of terms and conditions that conflict with the terms and conditions providing in the RFP or in any subsequent addendum may be rejected without further consideration.

3.9.2 Offer Form, Page OF-1. Offer Form, OF-1 is required to be completed using Offeror's exact legal name as registered with the Department of Commerce and Consumer Affairs, if applicable, in the appropriate space on Offer Form, OF-1 (SECTION SEVEN, Attachment 1). Failure to do so may delay proper execution of the Contract.

The Offeror's authorized signature on the Offer Form, OF-1 shall be an original signature in ink, which shall be required before an award, if any, can be made. The submission of the proposal shall indicate Offeror's intent to be bound.

3.9.3 Offer Form, Page OF-2. Pricing shall be submitted on Offer Form OF-2 (SECTION SEVEN, Attachment 2). The price shall be the all-inclusive cost, including the GET, to the State. No other costs will be honored. Any unit prices shall be inclusive.

3.10 PROPOSAL CONTENTS

Proposals must:

3.10.1 Include a transmittal letter to confirm that the Offeror shall comply with the requirements, provisions, terms, and conditions specified in this RFP.

3.10.2 Include a signed Offer Form OF-1 with the complete name and address of Offeror's firm and the name, mailing address, telephone number, and fax number of the person the State should contact regarding the Offeror's proposal.

3.10.3 If subcontractor(s) will be used, append a statement to the transmittal letter from each subcontractor, signed by an individual authorized to legally bind the subcontractor and stating:

a. The general scope of work to be performed by the subcontractor;

b. The subcontractor's willingness to perform for the indicated.

3.10.4 Provide all of the information requested in this RFP in the order specified.

3.10.5 Be organized into sections, following the exact format using all titles, subtitles, and numbering, with tabs separating each section described below. Each section must be addressed individually and pages must be numbered.

a. Transmittal Letter
See SECTION SEVEN, Attachment 1, Offer Form OF-1.

b. Experience and Capabilities.

1) A complete, relevant, and current client listing.

2) The number of years Offeror has been in business and the number of years Offeror has performed services specified by this RFP.

3) A list of key personnel and associated resumes for those who will be dedicated to this project.

4) A list of at least three (3) references from the Offeror's client listing that may be contacted by the State as to the Offeror's past and current job performance. Offeror shall provide names, titles, organizations, telephone numbers, email and postal addresses.

5) A summary listing of judgments or pending lawsuits or actions against; adverse contract actions, including termination(s), suspension, imposition of penalties, or other actions relating to failure to perform or deficiencies in fulfilling contractual obligations against your firm. If none, so state.

6) A list of sample projects and/or examples of written plans.

c. Proposal including an overall strategy, timeline and plan.

d. Pricing.
See SECTION SEVEN, Attachment 2, Offer Form OF-2.

e. Exceptions.

3.11 RECEIPT AND REGISTER OF PROPOSALS

Proposals will be received at the State of Hawai'i Department of Defense, Engineering Office, located in Building 306-A, Room 228, 3949 Diamond Head Road, Honolulu, Hawai'i 96816-4495 and receipt verified by procurement officials no later than date specified in Section One, or as amended.

If Offeror chooses to have proposal delivered by the United States Postal Service (USPS), please be aware that the USPS does not deliver directly to the Engineering Office, but to a central mailroom. This may cause a delay and the offeror's proposal may not reach the Engineering Office in time and/or after deadline, resulting in automatic rejection.

The register of proposals and proposals of the Offeror(s) shall be open to public inspection upon posting of award pursuant to section 103D-701, HRS.

3.12 BEST AND FINAL OFFER (BAFO)

If the State determines a BAFO is necessary, it shall request one from the Offeror. The Offeror shall submit its BAFO and any BAFO received after the deadline or not received shall not be considered.

3.13 MODIFICATION PRIOR TO SUBMITTAL DEADLINE OR WITHDRAWAL OF OFFERS

3.13.1 The Offeror may modify or withdraw a proposal before the proposal due date and time.

3.13.2 Any change, addition, deletion of attachment(s) or data entry of an Offer may be made prior to the deadline for submittal of offers.

3.14 MISTAKES IN PROPOSALS

3.14.1 Mistakes shall not be corrected after award of contract.

3.14.2 When the Procurement Officer knows or has reason to conclude before award that a mistake has been made, the Procurement Officer should request the offeror to confirm the proposal. If the Offeror alleges mistake, the proposal may be corrected or withdrawn pursuant to this section.

3.14.3 Once discussions are commenced or after best and final offers are requested, any priority-listed Offeror may freely correct any mistake by modifying or withdrawing the proposal until the time and date set for receipt of best and final offers.

3.14.4 If discussions are not held, or if the best and final offers upon which award will be made have been received, mistakes shall be corrected to the intended correct offer whenever the mistake and the intended correct offer are clearly evident on the face of the proposal, in which event the proposal may not be withdrawn.

3.14.5 If discussions are not held, or if the best and final offers upon which award will be made have been received, an Offeror alleging a material mistake of fact which makes a proposal non-responsive may be permitted to withdraw the proposal if: the mistake is clearly evident on the face of the proposal but the intended correct offer is not; or the Offeror submits evidence which clearly and convincingly demonstrates that a mistake was made.

Technical irregularities are matters of form rather than substance evident from the proposal document, or insignificant mistakes that can be waived or corrected without prejudice to other Offerors; that is, when there is no effect on price, quality, or quantity. If discussions are not held or if best and final offers upon which award will be made have been received, the Procurement Officer may waive such irregularities or allow an Offeror to correct them if either is in the best interest of the State. Examples include the failure of an Offeror to: return the number of signed proposals required by the request for proposals; sign the proposal, but only if the unsigned proposal is

accompanied by other material indicating the Offeror's intent to be bound; or to acknowledge receipt of an amendment to the request for proposal, but only if it is clear from the proposal that the Offeror received the amendment and intended to be bound by its terms; or the amendment involved had no effect on price, quality or quantity.

SECTION FOUR

EVALUATION CRITERIA

Evaluation criteria and the associated points are listed below. The award will be made to the responsible Offeror whose proposal is determined to be the most advantageous to the State based on the evaluation criteria listed in this section.

The total number of points used to score this contract is 100.

1. Competitiveness and Reasonableness of Price (total **10** points)

2. Previous experience, capability, and proficiency in the following: (total **35** points)

    A. Offeror's Overall Project Approach/Business Solution (**10** points)
    The Offeror's approach and comprehensiveness of the proposal as it relates to the services requested in Section 2.2, Scope of Work B. Objectives, including the development of the plan/annex/checklist and use of synchronization matrix as a method of planning.

    B. Offeror Organization and Staffing (**25** points)
    - Experience of key personnel assigned to the project (including professional work experience in Hawai'i and years of hands-on experience with emergency management planning and specialized planning expertise.
    - Evidence that at least one person tasked to the project maintains a security clearance. Offeror experience working with federal, state, and private sector entities

3. Sample projects and/or examples of written plans, organizational charts, company's contact directory, etc. (total 5 points)

4. Past Performance on Projects of Similar Scope for Public Agencies or Private Industry in Hawai'i (total **35** points)

    A. Number of years in the business and the number of years performing services specified in the RFP, to include specialized planning expertise in the areas of planning activities, and emergency management

5. Project Proposal (total **15** points)

    A. Demonstrated ability to complete awarded work within allotted time. (Has Offeror failed to complete any awarded work, e.g. terminated for default or failed to complete a contact in the last five (5) years. (5 points)

    B. Development of documents (plan, annex, checklist) based on state and county requirements. (5 points)

    C. Offeror must identify planning methodology for successful plan development. (5 points)

SECTION FIVE

CONTRACTOR SELECTION AND CONTRACT AWARD

5.1 EVALUATION OF PROPOSALS

The Procurement Officer, or an evaluation committee of at least three (3) qualified State employees selected by the Procurement Officer, shall evaluate proposals. The evaluation will be based solely on the evaluation criteria set out in Section Four of this RFP.

Prior to holding any discussion, a priority list shall be generated consisting of offers determined to be acceptable or potentially acceptable. However, proposals may be accepted without such discussions.

If numerous acceptable and potentially acceptable proposals are submitted, the evaluation committee may limit the priority list to the three highest ranked, responsible Offerors.

5.2 DISCUSSION WITH PRIORITY LISTED OFFERORS

The State may invite priority listed Offerors to discuss with their proposals to ensure thorough, mutual understanding. The State in its sole discretion shall schedule the time and location for these discussions, generally within the timeframe indicated in *RFP Schedule and Significant Dates.* The State may also conduct discussions with priority listed Offerors to clarify issues regarding the proposals before requesting Best and Final Offers, if necessary.

5.3 AWARD OF CONTRACT

Method of Award. Award will be made to the responsible Offeror whose proposal is determined to be the most advantageous to the State based on the evaluation criteria set forth in the RFP.

5.4 RESPONSIBILITY OF OFFERORS

Offeror is advised that in order to be awarded a contract under this solicitation, Offeror will be required, to be compliant with all laws governing entities doing business in the State including the following chapters and pursuant to HRS §103D-310(c):

1. Chapter 237, General Excise Tax Law;
2. Chapter 383, Hawai'i Employment Security Law;
3. Chapter 386, Worker's Compensation Law;
4. Chapter 392, Temporary Disability Insurance;
5. Chapter 393, Prepaid Health Care Act; and
6. §103D-310(c), Certificate of Good Standing (COGS) for entities doing business in the State.

The State will verify compliance on Hawai'i Compliance Express (HCE).

Hawai'i Compliance Express. The HCE is an electronic system that allows vendors/contractors/service providers doing business with the State to quickly and easily demonstrate compliance with applicable laws. It is an online system that replaces the necessity of obtaining paper compliance certificates from the Department of Taxation, Federal Internal Revenue Service, Department of Labor and Industrial Relations, and Department of Commerce and Consumer Affairs.

Vendors/contractors/service providers should register with (HCE) prior to submitting an offer at https://vendors.ehawaii.gov. The annual registration fee is $12.00 and the 'Certificate of Vendor Compliance' is accepted for the execution of contract and final payment.

Timely Registration on HCE. Vendors/contractors/service providers are advised to register on HCE soon as possible. If a vendor/contractor/service provider is not compliant on HCE at the time of award, an Offeror will not receive the award.

5.5 PROPOSAL AS PART OF THE CONTRACT

This RFP and all or part of the successful proposal may be incorporated into the contract.

5.6 PUBLIC EXAMINATION OF PROPOSALS

Except for confidential portions, the proposals shall be made available for public inspection upon posting of award pursuant to HRS §103D-701.

If a person is denied access to a State procurement record, the person may appeal the denial to the office of information practices in accordance with HRS §92F-42(12).

5.7 DEBRIEFING

Pursuant to HAR §3-122-60, a non-selected Offeror may request a debriefing to understand the basis for award.

A written request for debriefing shall be made within three (3) working days after the posting of the award of the contract. The Procurement Officer or designee shall hold the debriefing within seven (7) working days to the extent practicable from the receipt date of written request.

Any protest by the requestor following a debriefing, shall be filed within five (5) working days, as specified in HAR §103D-303(h).

5.8 PROTEST PROCEDURES

Pursuant to HRS §103D-701 and HAR §3-126-3, an actual or prospective Offeror who is aggrieved in connection with the solicitation or award of a contract may submit a protest. Any protest shall be submitted in writing to the Procurement Officer at:

STATE DEPARTMENT OF DEFENSE
Engineering Office
3949 DIAMOND HEAD ROAD, ROOM 228
Honolulu, Hawai'i 96816-4495
Attention: Theasius Allen

A protest shall be submitted in writing within five (5) working days after the aggrieved person knows or should have known of the facts giving rise thereto; provided that a protest based upon the content of the solicitation shall be submitted in writing prior to the date set for receipt of offers. Further provided that a protest of an award or proposed award shall be submitted within five (5) working days after the posting of award or if requested, within five (5) working days after the PO's debriefing was completed.

The notice of award, if any, resulting from this solicitation shall be posted on the Hawai'i Awards & Notices Data System (HANDS), which is available on the SPO website: http://hands.ehawaii.gov/hands/welcome.

5.9 APPROVALS

Any agreement arising out of this offer may be subject to the approval of the Department of the Attorney General, and to all further approvals, including the approval of the Governor, as required by statute, regulation, rule, order, or other directive.

5.10 CONTRACT EXECUTION

Successful Offeror receiving award shall enter into a formal written contract in the form as in Exhibit B. No performance or payment bond is required for this contract.

No work is to be undertaken by the Contractor prior to the effective date of contract. The State of Hawai'i is not liable for any work, contract, costs, expenses, loss of profits, or any damages whatsoever incurred by the Contractor prior to the official starting date.

If an option to extend is mutually agreed upon, the Contractor shall be required to execute a supplement to the contract for the additional extension period.

5.11 INSURANCE

5.11.1 Prior to the contract start date, the Contractor shall procure at its sole expense and maintain insurance coverage acceptable to the State in full force and effect throughout the term of the Contract. The Offeror shall provide proof of insurance for the following minimum insurance coverage(s) and limit(s) in order to be awarded a contract. The type of insurance coverage is listed as follows:

1. Commercial General Liability Insurance

Commercial general liability insurance coverage against claims for bodily injury and property damage arising out of all operations, activities or contractual liability by the Contractor, its employees and subcontractors during the term of the Contract. This insurance shall include the following coverage and limits specified or required by any applicable law: bodily injury and property damage coverage with a minimum of $1,000,000 per occurrence; personal and advertising injury of $1,000,000 per occurrence;

broadcasters' liability insurance of $1,000,000 per occurrence; and with an aggregated limit of $2,000,000. The commercial general liability policy shall be written on an occurrence basis and the policy shall provide legal defense costs and expenses in addition to the limits of liability stated above. The Contractor shall be responsible for payment of any deductible applicable to this policy.

2. Automobile Liability Insurance

   Automobile liability insurance covering owned, non-owned, leased, and hired vehicles with a minimum of $1,000,000 for bodily injury for each person, $1,000,000 for bodily injury for each accident, and $1,000,000 for property damage for each accident.

3. Appropriate levels of per occurrence insurance coverage for workers' compensation and any other insurance coverage required by Federal or State law.

5.11.2 The Contractor shall deposit with the SPO, on or before the effective date of the Contract, certificate(s) of insurance necessary to satisfy the SPO that the provisions of the Contract have been complied with, and to keep such insurance in effect and provide the certificate(s) of insurance to the SPO during the entire term of the Contract. Upon request by the SPO, the Contractor shall furnish a copy of the policy or policies.

5.11.3 The Contractor will immediately provide written notice to the SPO and the State of Hawai'i Department of Defense, Engineering Office should any of the insurance policies evidenced on its Certificate of Insurance form be cancelled, limited in scope, or not renewed up expiration.

5.11.4 The certificates of insurance shall contain the following clauses:

1. "The State of Hawai'i is added as an additional insured as respects to operations performed for the State of Hawai'i."

2. "It is agreed that any insurance maintained by the State of Hawai'i will apply in excess of, and not contribute with, insurance provided by this policy."

5.11.5. Failure of the Contractor to provide and keep in force such insurance shall constitute a material default under the Contract, entitling the State to exercise any or all of the remedies provided in the Contract (including without limitation terminating the Contract). The procuring of any required policy or policies of insurance shall not be construed to limit the Contractor's liability hereunder, or to fulfill the indemnification provisions of the Contract. Notwithstanding said policy or policies of insurance, the Contractor shall be responsible for the full and total amount of any damage, injury, or loss caused by the Contractor's negligence or neglect in the provision of services under the Contract.

5.12 REQUIREMENTS FOR PERFORMANCE BONDS

A performance bond is not required for this solicitation.

5.13 INVOICING AND PAYMENT

Incremental payments shall be made to the awarded Contractor on a quarterly basis, upon receipt of reports that meet the expectations of the RFP. The receipt of quarterly reports shall be due based on the timeline submitted by the Contractor in the proposal, or as amended.

Invoices can be processed at quarterly during the contract period. The following information will need to be in the invoice.

- Reference the project name
- Reference Contract Number
- Provide services performed

Invoices can be sent electronically via email at: glen.m.badua@hawaii.gov

The Hawai'i State Department of Defense, Office of Homeland Security will make payments via checks. Electronic deposits are not allowed.

Payment processing times takes approximately 3-4 weeks for a check to be issued. Checks are mailed via certified mail, unless instructed by the contractor to deliver via an alternative method.

5.14 CONTRACT INVALIDATION

If any provision of this contract is found to be invalid, such invalidation will not be construed to invalidate the entire contract.

SECTION SIX

SPECIAL PROVISIONS

6.1 OFFER GUARANTY

A proposal security deposit is NOT required for this RFP.

6.2 ACCEPTANCE AND TESTING

Final acceptance of the project will be provided upon delivery of all named project deliverables, including any required DOD/County revisions/changes.

6.3 INTELLECTUAL PROPERTY RIGHTS

The State reserves the right to unlimited, irrevocable, worldwide, perpetual, royalty-free, non-exclusive licenses to use, modify, reproduce, perform, release, display, create derivative works from, and disclose the work product, and to transfer the intellectual property to third parties for State purposes.

6.4 WARRANTIES AND DISCLAIMER OF IMPLIED WARRANTIES

Warranty for all plans shall be for the period of one year from the date of final acceptance of the plans. All defects identified during the 1-year warranty period shall be corrected within 5 days from notice of the defect or issue.

6.5 TERMINATIONS FOR CONVENIENCE OR UNAVAILABILITY OF FUNDS

Clarify conditions when funds are limited but assurance of payment for completed performance.

SECTION SEVEN

ATTACHMENTS AND EXHIBITS

- Attachment 1: OFFER FORM, OF-1
- Attachment 2: OFFER FORM, OF-2
- Exhibit A: GENERAL PROVISIONS
- Exhibit B: AG GENERAL CONDITIONS
- Exhibit C: OVERVIEW OF THE RFP PROCESS
- Exhibit D: REFERENCE MATERIALS
  - D1: Targeted Violence Prevention Strategy
  - D2: Department of Homeland Security's Infrastructure Resilience Planning Framework
  - D3: Cyber Disruption Response Plan
  - D4: 2022 State and Local Cybersecurity Grant Program (SLCGP)

OFFER FORM
PLAN DEVELOPMENT AND SUPPORTING ACTIVITIES, STATE OF HAWAI'I,
DEPARTMENT OF DEPARTMENT OF DEFENSE, OFFICE OF HOMELAND SECURITY
Job No. RFP-CA-202212

Adjutant General
State of Hawai'i Department of Defense
3949 Diamond Head Road
Honolulu, Hawai'i 96816-4495

Dear Sir:

The undersigned has carefully read and understands the terms and conditions specified in the Specifications and Special Provisions attached hereto, and in the General Conditions, by reference made a part hereof and available upon request; and hereby submits the following offer to perform the work specified herein, all in accordance with the true intent and meaning thereof. The undersigned further understands and agrees that by submitting this offer, 1) he/she is declaring his/her offer is not in violation of Chapter 84, Hawai'i Revised Statutes, concerning prohibited State contracts, and 2) he/she is certifying that the price(s) submitted was (were) independently arrived at without collusion.

Offeror is:
☐ Sole Proprietor ☐ Partnership ☐ *Corporation ☐ Joint Venture
☐ Other _____
*State of incorporation: _____

Hawai'i General Excise Tax License I.D. No. _____
Federal I.D. No. _____

Payment address (other than street address below): _____
City, State, Zip Code: _____

Business address (street address): _____
City, State, Zip Code: _____

Respectfully submitted:

Date: _____ **(x)** _____
Authorized (Original) Signature

Telephone No.: _____

_____
Fax No.: _____ Name and Title (Please Type or Print)

E-mail Address: * _____
_____ **Exact Legal Name of Company (Offeror) (**2)**

(*1) Original signature in ink. If unsigned or the affixed signature is a facsimile or a photocopy, the offer shall be automatically rejected unless accompanied by other material, containing an original signature, indicating the Offeror's intent to be bound.

(**2) If Offeror is a "dba" or a "division" of a corporation, furnish the exact legal name of the corporation under which the awarded contract will be executed:

OFFER FORM
OF-2

Total contract cost for accomplishing the development and delivery of the services.

_____

_____ DOLLAR ($_____).

{*BIDDER'S INSTRUCTIONS: Fill in the total dollar cost in numbers and write out the total dollar in words. Prices shall be written in ink or typed.}*

Note: Pricing shall include labor, materials, supplies, all applicable taxes, and any other costs incurred to provide the specified services.

Offeror _____
Name of Company

GENERAL CONDITIONS

Table of Contents

1. Coordination of Services by the STATE. The head of the purchasing agency ("HOPA") (which term includes the designee of the HOPA) shall coordinate the services to be provided by the CONTRACTOR in order to complete the performance required in the Contract. The CONTRACTOR shall maintain communications with HOPA at all stages of the CONTRACTOR'S work, and submit to HOPA for resolution any questions which may arise as to the performance of this Contract. "Purchasing agency" as used in these General Conditions means and includes any governmental body which is authorized under chapter 103D, HRS, or its implementing rules and procedures, or by way of delegation, to enter into contracts for the procurement of goods or services or both.

2. Relationship of Parties: Independent Contractor Status and Responsibilities, Including Tax Responsibilities.

   a. In the performance of services required under this Contract, the CONTRACTOR is an "independent contractor," with the authority and responsibility to control and direct the performance and details of the work and services required under this Contract; however, the STATE shall have a general right to inspect work in progress to determine whether, in the STATE'S opinion, the services are being performed by the CONTRACTOR in compliance with this Contract. Unless otherwise provided by special condition, it is understood that the STATE does not agree to use the CONTRACTOR exclusively, and that the CONTRACTOR is free to contract to provide services to other individuals or entities while under contract with the STATE.

   b. The CONTRACTOR and the CONTRACTOR'S employees and agents are not by reason of this Contract, agents or employees of the State for any purpose, and the CONTRACTOR and the CONTRACTOR'S employees and agents shall not be entitled to claim or receive from the State any vacation, sick leave, retirement, workers' compensation, unemployment insurance, or other benefits provided to state employees.

   c. The CONTRACTOR shall be responsible for the accuracy, completeness, and adequacy of the CONTRACTOR'S performance under this Contract. Furthermore, the CONTRACTOR intentionally, voluntarily, and knowingly assumes the sole and entire liability to the CONTRACTOR'S employees and agents, and to any individual not a party to this Contract, for all loss, damage, or injury caused by the CONTRACTOR, or the CONTRACTOR'S employees or agents in the course of their employment.

   d. The CONTRACTOR shall be responsible for payment of all applicable federal, state, and county taxes and fees which may become due and owing by the CONTRACTOR by reason of this Contract, including but not limited to (i) income taxes, (ii) employment related fees, assessments, and taxes, and (iii) general excise taxes. The CONTRACTOR also is responsible for obtaining all licenses, permits, and certificates that may be required in order to perform this Contract.

   e. The CONTRACTOR shall obtain a general excise tax license from the Department of Taxation, State of Hawaii, in accordance with section 237-9, HRS, and shall comply with all requirements thereof. The CONTRACTOR shall obtain a tax clearance certificate from the Director of Taxation, State of Hawaii, and the Internal Revenue Service, U.S. Department of the Treasury, showing that all delinquent taxes, if any, levied or accrued under state law and the Internal Revenue Code of 1986, as amended, against the CONTRACTOR have been paid and submit the same to the STATE prior to commencing any performance under this Contract. The CONTRACTOR shall also be solely responsible for meeting all requirements necessary to obtain the tax clearance certificate required for final payment under sections 103-53 and 103D-328, HRS, and paragraph 17 of these General Conditions.

   f. The CONTRACTOR is responsible for securing all employee-related insurance coverage for the CONTRACTOR and the CONTRACTOR'S employees and agents that is or may be required by law, and for payment of all premiums, costs, and other liabilities associated with securing the insurance coverage.

g. The CONTRACTOR shall obtain a certificate of compliance issued by the Department of Labor and Industrial Relations, State of Hawaii, in accordance with section103D-310, HRS, and section 3-122-112, HAR, that is current within six months of the date of issuance.

h. The CONTRACTOR shall obtain a certificate of good standing issued by the Department of Commerce and Consumer Affairs, State of Hawaii, in accordance with section 103D-310, HRS, and section 3-122-112, HAR, that is current within six months of the date of issuance.

i. In lieu of the above certificates from the Department of Taxation, Labor and Industrial Relations, and Commerce and Consumer Affairs, the CONTRACTOR may submit proof of compliance through the State Procurement Office's designated certification process.

3. Personnel Requirements.

a. The CONTRACTOR shall secure, at the CONTRACTOR'S own expense, all personnel required to perform this Contract.

b. The CONTRACTOR shall ensure that the CONTRACTOR'S employees or agents are experienced and fully qualified to engage in the activities and perform the services required under this Contract, and that all applicable licensing and operating requirements imposed or required under federal, state, or county law, and all applicable accreditation and other standards of quality generally accepted in the field of the activities of such employees and agents are complied with and satisfied.

4. Nondiscrimination. No person performing work under this Contract, including any subcontractor, employee, or agent of the CONTRACTOR, shall engage in any discrimination that is prohibited by any applicable federal, state, or county law.

5. Conflicts of Interest. The CONTRACTOR represents that neither the CONTRACTOR, nor any employee or agent of the CONTRACTOR, presently has any interest, and promises that no such interest, direct or indirect, shall be acquired, that would or might conflict in any manner or degree with the CONTRACTOR'S performance under this Contract.

6. Subcontracts and Assignments. The CONTRACTOR shall not assign or subcontract any of the CONTRACTOR'S duties, obligations, or interests under this Contract and no such assignment or subcontract shall be effective unless (i) the CONTRACTOR obtains the prior written consent of the STATE, and (ii) the CONTRACTOR'S assignee or subcontractor submits to the STATE a tax clearance certificate from the Director of Taxation, State of Hawaii, and the Internal Revenue Service, U.S. Department of Treasury, showing that all delinquent taxes, if any, levied or accrued under state law and the Internal Revenue Code of 1986, as amended, against the CONTRACTOR'S assignee or subcontractor have been paid. Additionally, no assignment by the CONTRACTOR of the CONTRACTOR'S right to compensation under this Contract shall be effective unless and until the assignment is approved by the Comptroller of the State of Hawaii, as provided in section 40-58, HRS.

a. Recognition of a successor in interest. When in the best interest of the State, a successor in interest may be recognized in an assignment contract in which the STATE, the CONTRACTOR and the assignee or transferee (hereinafter referred to as the "Assignee") agree that:

(1) The Assignee assumes all of the CONTRACTOR'S obligations;

(2) The CONTRACTOR remains liable for all obligations under this Contract but waives all rights under this Contract as against the STATE; and

(3) The CONTRACTOR shall continue to furnish, and the Assignee shall also furnish, all required bonds.

b. Change of name. When the CONTRACTOR asks to change the name in which it holds this Contract with the STATE, the procurement officer of the purchasing agency (hereinafter referred to as the "Agency procurement officer") shall, upon receipt of a document acceptable or satisfactory to the

Agency procurement officer indicating such change of name (for example, an amendment to the CONTRACTOR'S articles of incorporation), enter into an amendment to this Contract with the CONTRACTOR to effect such a change of name. The amendment to this Contract changing the CONTRACTOR'S name shall specifically indicate that no other terms and conditions of this Contract are thereby changed.

c. Reports. All assignment contracts and amendments to this Contract effecting changes of the CONTRACTOR'S name or novations hereunder shall be reported to the chief procurement officer (CPO) as defined in section 103D-203(a), HRS, within thirty days of the date that the assignment contract or amendment becomes effective.

d. Actions affecting more than one purchasing agency. Notwithstanding the provisions of subparagraphs 6a through 6c herein, when the CONTRACTOR holds contracts with more than one purchasing agency of the State, the assignment contracts and the novation and change of name amendments herein authorized shall be processed only through the CPO's office.

7. Indemnification and Defense. The CONTRACTOR shall defend, indemnify, and hold harmless the State of Hawaii, the contracting agency, and their officers, employees, and agents from and against all liability, loss, damage, cost, and expense, including all attorneys' fees, and all claims, suits, and demands therefore, arising out of or resulting from the acts or omissions of the CONTRACTOR or the CONTRACTOR'S employees, officers, agents, or subcontractors under this Contract. The provisions of this paragraph shall remain in full force and effect notwithstanding the expiration or early termination of this Contract.

8. Cost of Litigation. In case the STATE shall, without any fault on its part, be made a party to any litigation commenced by or against the CONTRACTOR in connection with this Contract, the CONTRACTOR shall pay all costs and expenses incurred by or imposed on the STATE, including attorneys' fees.

9. Liquidated Damages. When the CONTRACTOR is given notice of delay or nonperformance as specified in paragraph 13 (Termination for Default) and fails to cure in the time specified, it is agreed the CONTRACTOR shall pay to the STATE the amount, if any, set forth in this Contract per calendar day from the date set for cure until either (i) the STATE reasonably obtains similar goods or services, or both, if the CONTRACTOR is terminated for default, or (ii) until the CONTRACTOR provides the goods or services, or both, if the CONTRACTOR is not terminated for default. To the extent that the CONTRACTOR'S delay or nonperformance is excused under paragraph 13d (Excuse for Nonperformance or Delay Performance), liquidated damages shall not be assessable against the CONTRACTOR. The CONTRACTOR remains liable for damages caused other than by delay.

10. STATE'S Right of Offset. The STATE may offset against any monies or other obligations the STATE owes to the CONTRACTOR under this Contract, any amounts owed to the State of Hawaii by the CONTRACTOR under this Contract or any other contracts, or pursuant to any law or other obligation owed to the State of Hawaii by the CONTRACTOR, including, without limitation, the payment of any taxes or levies of any kind or nature. The STATE will notify the CONTRACTOR in writing of any offset and the nature of such offset. For purposes of this paragraph, amounts owed to the State of Hawaii shall not include debts or obligations which have been liquidated, agreed to by the CONTRACTOR, and are covered by an installment payment or other settlement plan approved by the State of Hawaii, provided, however, that the CONTRACTOR shall be entitled to such exclusion only to the extent that the CONTRACTOR is current with, and not delinquent on, any payments or obligations owed to the State of Hawaii under such payment or other settlement plan.

11. Disputes. Disputes shall be resolved in accordance with section 103D-703, HRS, and chapter 3-126, Hawaii Administrative Rules ("HAR"), as the same may be amended from time to time.

12. Suspension of Contract. The STATE reserves the right at any time and for any reason to suspend this Contract for any reasonable period, upon written notice to the CONTRACTOR in accordance with the provisions herein.

a. Order to stop performance. The Agency procurement officer may, by written order to the CONTRACTOR, at any time, and without notice to any surety, require the CONTRACTOR to stop all or any part of the performance called for by this Contract. This order shall be for a specified

period not exceeding sixty (60) days after the order is delivered to the CONTRACTOR, unless the parties agree to any further period. Any such order shall be identified specifically as a stop performance order issued pursuant to this section. Stop performance orders shall include, as appropriate: (1) A clear description of the work to be suspended; (2) Instructions as to the issuance of further orders by the CONTRACTOR for material or services; (3) Guidance as to action to be taken on subcontracts; and (4) Other instructions and suggestions to the CONTRACTOR for minimizing costs. Upon receipt of such an order, the CONTRACTOR shall forthwith comply with its terms and suspend all performance under this Contract at the time stated, provided, however, the CONTRACTOR shall take all reasonable steps to minimize the occurrence of costs allocable to the performance covered by the order during the period of performance stoppage. Before the stop performance order expires, or within any further period to which the parties shall have agreed, the Agency procurement officer shall either:

(1) Cancel the stop performance order; or

(2) Terminate the performance covered by such order as provided in the termination for default provision or the termination for convenience provision of this Contract.

b. Cancellation or expiration of the order. If a stop performance order issued under this section is cancelled at any time during the period specified in the order, or if the period of the order or any extension thereof expires, the CONTRACTOR shall have the right to resume performance. An appropriate adjustment shall be made in the delivery schedule or contract price, or both, and the Contract shall be modified in writing accordingly, if:

(1) The stop performance order results in an increase in the time required for, or in the CONTRACTOR'S cost properly allocable to, the performance of any part of this Contract; and

(2) The CONTRACTOR asserts a claim for such an adjustment within thirty (30) days after the end of the period of performance stoppage; provided that, if the Agency procurement officer decides that the facts justify such action, any such claim asserted may be received and acted upon at any time prior to final payment under this Contract.

c. Termination of stopped performance. If a stop performance order is not cancelled and the performance covered by such order is terminated for default or convenience, the reasonable costs resulting from the stop performance order shall be allowable by adjustment or otherwise.

d. Adjustment of price. Any adjustment in contract price made pursuant to this paragraph shall be determined in accordance with the price adjustment provision of this Contract.

13. Termination for Default.

a. Default. If the CONTRACTOR refuses or fails to perform any of the provisions of this Contract with such diligence as will ensure its completion within the time specified in this Contract, or any extension thereof, otherwise fails to timely satisfy the Contract provisions, or commits any other substantial breach of this Contract, the Agency procurement officer may notify the CONTRACTOR in writing of the delay or non-performance and if not cured in ten (10) days or any longer time specified in writing by the Agency procurement officer, such officer may terminate the CONTRACTOR'S right to proceed with the Contract or such part of the Contract as to which there has been delay or a failure to properly perform. In the event of termination in whole or in part, the Agency procurement officer may procure similar goods or services in a manner and upon the terms deemed appropriate by the Agency procurement officer. The CONTRACTOR shall continue performance of the Contract to the extent it is not terminated and shall be liable for excess costs incurred in procuring similar goods or services.

b. CONTRACTOR'S duties. Notwithstanding termination of the Contract and subject to any directions from the Agency procurement officer, the CONTRACTOR shall take timely, reasonable, and

necessary action to protect and preserve property in the possession of the CONTRACTOR in which the STATE has an interest.

c. Compensation. Payment for completed goods and services delivered and accepted by the STATE shall be at the price set forth in the Contract. Payment for the protection and preservation of property shall be in an amount agreed upon by the CONTRACTOR and the Agency procurement officer. If the parties fail to agree, the Agency procurement officer shall set an amount subject to the CONTRACTOR'S rights under chapter 3-126, HAR. The STATE may withhold from amounts due the CONTRACTOR such sums as the Agency procurement officer deems to be necessary to protect the STATE against loss because of outstanding liens or claims and to reimburse the STATE for the excess costs expected to be incurred by the STATE in procuring similar goods and services.

d. Excuse for nonperformance or delayed performance. The CONTRACTOR shall not be in default by reason of any failure in performance of this Contract in accordance with its terms, including any failure by the CONTRACTOR to make progress in the prosecution of the performance hereunder which endangers such performance, if the CONTRACTOR has notified the Agency procurement officer within fifteen (15) days after the cause of the delay and the failure arises out of causes such as: acts of God; acts of a public enemy; acts of the State and any other governmental body in its sovereign or contractual capacity; fires; floods; epidemics; quarantine restrictions; strikes or other labor disputes; freight embargoes; or unusually severe weather. If the failure to perform is caused by the failure of a subcontractor to perform or to make progress, and if such failure arises out of causes similar to those set forth above, the CONTRACTOR shall not be deemed to be in default, unless the goods and services to be furnished by the subcontractor were reasonably obtainable from other sources in sufficient time to permit the CONTRACTOR to meet the requirements of the Contract. Upon request of the CONTRACTOR, the Agency procurement officer shall ascertain the facts and extent of such failure, and, if such officer determines that any failure to perform was occasioned by any one or more of the excusable causes, and that, but for the excusable cause, the CONTRACTOR'S progress and performance would have met the terms of the Contract, the delivery schedule shall be revised accordingly, subject to the rights of the STATE under this Contract. As used in this paragraph, the term "subcontractor" means subcontractor at any tier.

e. Erroneous termination for default. If, after notice of termination of the CONTRACTOR'S right to proceed under this paragraph, it is determined for any reason that the CONTRACTOR was not in default under this paragraph, or that the delay was excusable under the provisions of subparagraph 13d, "Excuse for nonperformance or delayed performance," the rights and obligations of the parties shall be the same as if the notice of termination had been issued pursuant to paragraph 14.

f. Additional rights and remedies. The rights and remedies provided in this paragraph are in addition to any other rights and remedies provided by law or under this Contract.

14. Termination for Convenience.

a. Termination. The Agency procurement officer may, when the interests of the STATE so require, terminate this Contract in whole or in part, for the convenience of the STATE. The Agency procurement officer shall give written notice of the termination to the CONTRACTOR specifying the part of the Contract terminated and when termination becomes effective.

b. CONTRACTOR'S obligations. The CONTRACTOR shall incur no further obligations in connection with the terminated performance and on the date(s) set in the notice of termination the CONTRACTOR will stop performance to the extent specified. The CONTRACTOR shall also terminate outstanding orders and subcontracts as they relate to the terminated performance. The CONTRACTOR shall settle the liabilities and claims arising out of the termination of subcontracts and orders connected with the terminated performance subject to the STATE'S approval. The Agency procurement officer may direct the CONTRACTOR to assign the CONTRACTOR'S right, title, and interest under terminated orders or subcontracts to the STATE. The CONTRACTOR must still complete the performance not terminated by the notice of termination and may incur obligations as necessary to do so.

c. Right to goods and work product. The Agency procurement officer may require the CONTRACTOR to transfer title and deliver to the STATE in the manner and to the extent directed by the Agency procurement officer:

(1) Any completed goods or work product; and

(2) The partially completed goods and materials, parts, tools, dies, jigs, fixtures, plans, drawings, information, and contract rights (hereinafter called "manufacturing material") as the CONTRACTOR has specifically produced or specially acquired for the performance of the terminated part of this Contract.

The CONTRACTOR shall, upon direction of the Agency procurement officer, protect and preserve property in the possession of the CONTRACTOR in which the STATE has an interest. If the Agency procurement officer does not exercise this right, the CONTRACTOR shall use best efforts to sell such goods and manufacturing materials. Use of this paragraph in no way implies that the STATE has breached the Contract by exercise of the termination for convenience provision.

d. Compensation.

(1) The CONTRACTOR shall submit a termination claim specifying the amounts due because of the termination for convenience together with the cost or pricing data, submitted to the extent required by chapter 3-122, HAR, bearing on such claim. If the CONTRACTOR fails to file a termination claim within one year from the effective date of termination, the Agency procurement officer may pay the CONTRACTOR, if at all, an amount set in accordance with subparagraph 14d(3) below.

(2) The Agency procurement officer and the CONTRACTOR may agree to a settlement provided the CONTRACTOR has filed a termination claim supported by cost or pricing data submitted as required and that the settlement does not exceed the total Contract price plus settlement costs reduced by payments previously made by the STATE, the proceeds of any sales of goods and manufacturing materials under subparagraph 14c, and the Contract price of the performance not terminated.

(3) Absent complete agreement under subparagraph 14d(2) the Agency procurement officer shall pay the CONTRACTOR the following amounts, provided payments agreed to under subparagraph 14d(2) shall not duplicate payments under this subparagraph for the following:

(A) Contract prices for goods or services accepted under the Contract;

(B) Costs incurred in preparing to perform and performing the terminated portion of the performance plus a fair and reasonable profit on such portion of the performance, such profit shall not include anticipatory profit or consequential damages, less amounts paid or to be paid for accepted goods or services; provided, however, that if it appears that the CONTRACTOR would have sustained a loss if the entire Contract would have been completed, no profit shall be allowed or included and the amount of compensation shall be reduced to reflect the anticipated rate of loss;

(C) Costs of settling and paying claims arising out of the termination of subcontracts or orders pursuant to subparagraph 14b. These costs must not include costs paid in accordance with subparagraph 14d(3)(B);

(D) The reasonable settlement costs of the CONTRACTOR, including accounting, legal, clerical, and other expenses reasonably necessary for the preparation of settlement claims and supporting data with respect to the terminated portion of the Contract and for the termination of subcontracts thereunder, together with reasonable storage, transportation, and other costs incurred in connection with the protection or disposition of property allocable to the terminated portion of this Contract. The total sum to be paid the CONTRACTOR under this subparagraph shall not exceed the

total Contract price plus the reasonable settlement costs of the CONTRACTOR reduced by the amount of payments otherwise made, the proceeds of any sales of supplies and manufacturing materials under subparagraph 14d(2), and the contract price of performance not terminated.

(4) Costs claimed, agreed to, or established under subparagraphs 14d(2) and 14d(3) shall be in accordance with Chapter 3-123 (Cost Principles) of the Procurement Rules.

15. Claims Based on the Agency Procurement Officer's Actions or Omissions.

a. Changes in scope. If any action or omission on the part of the Agency procurement officer (which term includes the designee of such officer for purposes of this paragraph 15) requiring performance changes within the scope of the Contract constitutes the basis for a claim by the CONTRACTOR for additional compensation, damages, or an extension of time for completion, the CONTRACTOR shall continue with performance of the Contract in compliance with the directions or orders of such officials, but by so doing, the CONTRACTOR shall not be deemed to have prejudiced any claim for additional compensation, damages, or an extension of time for completion; provided:

(1) Written notice required. The CONTRACTOR shall give written notice to the Agency procurement officer:

(A) Prior to the commencement of the performance involved, if at that time the CONTRACTOR knows of the occurrence of such action or omission;

(B) Within thirty (30) days after the CONTRACTOR knows of the occurrence of such action or omission, if the CONTRACTOR did not have such knowledge prior to the commencement of the performance; or

(C) Within such further time as may be allowed by the Agency procurement officer in writing.

(2) Notice content. This notice shall state that the CONTRACTOR regards the act or omission as a reason which may entitle the CONTRACTOR to additional compensation, damages, or an extension of time. The Agency procurement officer, upon receipt of such notice, may rescind such action, remedy such omission, or take such other steps as may be deemed advisable in the discretion of the Agency procurement officer;

(3) Basis must be explained. The notice required by subparagraph 15a(1) describes as clearly as practicable at the time the reasons why the CONTRACTOR believes that additional compensation, damages, or an extension of time may be remedies to which the CONTRACTOR is entitled; and

(4) Claim must be justified. The CONTRACTOR must maintain and, upon request, make available to the Agency procurement officer within a reasonable time, detailed records to the extent practicable, and other documentation and evidence satisfactory to the STATE, justifying the claimed additional costs or an extension of time in connection with such changes.

b. CONTRACTOR not excused. Nothing herein contained, however, shall excuse the CONTRACTOR from compliance with any rules or laws precluding any state officers and CONTRACTOR from acting in collusion or bad faith in issuing or performing change orders which are clearly not within the scope of the Contract.

c. Price adjustment. Any adjustment in the price made pursuant to this paragraph shall be determined in accordance with the price adjustment provision of this Contract.

16. Costs and Expenses. Any reimbursement due the CONTRACTOR for per diem and transportation expenses under this Contract shall be subject to chapter 3-123 (Cost Principles), HAR, and the following guidelines:

a. Reimbursement for air transportation shall be for actual cost or coach class air fare, whichever is less.

b. Reimbursement for ground transportation costs shall not exceed the actual cost of renting an intermediate-sized vehicle.

c. Unless prior written approval of the HOPA is obtained, reimbursement for subsistence allowance (i.e., hotel and meals, etc.) shall not exceed the applicable daily authorized rates for inter-island or out-of-state travel that are set forth in the current Governor's Executive Order authorizing adjustments in salaries and benefits for state officers and employees in the executive branch who are excluded from collective bargaining coverage.

17. Payment Procedures; Final Payment; Tax Clearance.

a. Original invoices required. All payments under this Contract shall be made only upon submission by the CONTRACTOR of original invoices specifying the amount due and certifying that services requested under the Contract have been performed by the CONTRACTOR according to the Contract.

b. Subject to available funds. Such payments are subject to availability of funds and allotment by the Director of Finance in accordance with chapter 37, HRS. Further, all payments shall be made in accordance with and subject to chapter 40, HRS.

c. Prompt payment.

(1) Any money, other than retainage, paid to the CONTRACTOR shall be disbursed to subcontractors within ten (10) days after receipt of the money in accordance with the terms of the subcontract; provided that the subcontractor has met all the terms and conditions of the subcontract and there are no bona fide disputes; and

(2) Upon final payment to the CONTRACTOR, full payment to the subcontractor, including retainage, shall be made within ten (10) days after receipt of the money; provided that there are no bona fide disputes over the subcontractor's performance under the subcontract.

d. Final payment. Final payment under this Contract shall be subject to sections 103-53 and 103D-328, HRS, which require a tax clearance from the Director of Taxation, State of Hawaii, and the Internal Revenue Service, U.S. Department of Treasury, showing that all delinquent taxes, if any, levied or accrued under state law and the Internal Revenue Code of 1986, as amended, against the CONTRACTOR have been paid. Further, in accordance with section 3-122-112, HAR, CONTRACTOR shall provide a certificate affirming that the CONTRACTOR has remained in compliance with all applicable laws as required by this section.

18. Federal Funds. If this Contract is payable in whole or in part from federal funds, CONTRACTOR agrees that, as to the portion of the compensation under this Contract to be payable from federal funds, the CONTRACTOR shall be paid only from such funds received from the federal government, and shall not be paid from any other funds. Failure of the STATE to receive anticipated federal funds shall not be considered a breach by the STATE or an excuse for nonperformance by the CONTRACTOR.

19. Modifications of Contract.

a. In writing. Any modification, alteration, amendment, change, or extension of any term, provision, or condition of this Contract permitted by this Contract shall be made by written amendment to this Contract, signed by the CONTRACTOR and the STATE, provided that change orders shall be made in accordance with paragraph 20 herein.

b. No oral modification. No oral modification, alteration, amendment, change, or extension of any term, provision, or condition of this Contract shall be permitted.

c. Agency procurement officer. By written order, at any time, and without notice to any surety, the Agency procurement officer may unilaterally order of the CONTRACTOR:

(A) Changes in the work within the scope of the Contract; and

(B) Changes in the time of performance of the Contract that do not alter the scope of the Contract work.

d. Adjustments of price or time for performance. If any modification increases or decreases the CONTRACTOR'S cost of, or the time required for, performance of any part of the work under this Contract, an adjustment shall be made and this Contract modified in writing accordingly. Any adjustment in contract price made pursuant to this clause shall be determined, where applicable, in accordance with the price adjustment clause of this Contract or as negotiated.

e. Claim barred after final payment. No claim by the CONTRACTOR for an adjustment hereunder shall be allowed if written modification of the Contract is not made prior to final payment under this Contract.

f. Claims not barred. In the absence of a written contract modification, nothing in this clause shall be deemed to restrict the CONTRACTOR'S right to pursue a claim under this Contract or for a breach of contract.

g. Head of the purchasing agency approval. If this is a professional services contract awarded pursuant to section 103D-303 or 103D-304, HRS, any modification, alteration, amendment, change, or extension of any term, provision, or condition of this Contract which increases the amount payable to the CONTRACTOR by at least $25,000.00 and ten per cent (10%) or more of the initial contract price, must receive the prior approval of the head of the purchasing agency.

h. Tax clearance. The STATE may, at its discretion, require the CONTRACTOR to submit to the STATE, prior to the STATE'S approval of any modification, alteration, amendment, change, or extension of any term, provision, or condition of this Contract, a tax clearance from the Director of Taxation, State of Hawaii, and the Internal Revenue Service, U.S. Department of Treasury, showing that all delinquent taxes, if any, levied or accrued under state law and the Internal Revenue Code of 1986, as amended, against the CONTRACTOR have been paid.

i. Sole source contracts. Amendments to sole source contracts that would change the original scope of the Contract may only be made with the approval of the CPO. Annual renewal of a sole source contract for services should not be submitted as an amendment.

20. Change Order. The Agency procurement officer may, by a written order signed only by the STATE, at any time, and without notice to any surety, and subject to all appropriate adjustments, make changes within the general scope of this Contract in any one or more of the following:

(1) Drawings, designs, or specifications, if the goods or services to be furnished are to be specially provided to the STATE in accordance therewith;

(2) Method of delivery; or

(3) Place of delivery.

a. Adjustments of price or time for performance. If any change order increases or decreases the CONTRACTOR'S cost of, or the time required for, performance of any part of the work under this Contract, whether or not changed by the order, an adjustment shall be made and the Contract modified in writing accordingly. Any adjustment in the Contract price made pursuant to this provision shall be determined in accordance with the price adjustment provision of this Contract. Failure of the parties to agree to an adjustment shall not excuse the CONTRACTOR from proceeding with the Contract as changed, provided that the Agency procurement officer promptly and duly makes the provisional adjustments in payment or time for performance as may be reasonable. By

proceeding with the work, the CONTRACTOR shall not be deemed to have prejudiced any claim for additional compensation, or any extension of time for completion.

b. Time period for claim. Within ten (10) days after receipt of a written change order under subparagraph 20a, unless the period is extended by the Agency procurement officer in writing, the CONTRACTOR shall respond with a claim for an adjustment. The requirement for a timely written response by CONTRACTOR cannot be waived and shall be a condition precedent to the assertion of a claim.

c. Claim barred after final payment. No claim by the CONTRACTOR for an adjustment hereunder shall be allowed if a written response is not given prior to final payment under this Contract.

d. Other claims not barred. In the absence of a change order, nothing in this paragraph 20 shall be deemed to restrict the CONTRACTOR'S right to pursue a claim under the Contract or for breach of contract.

21. Price Adjustment.

a. Price adjustment. Any adjustment in the contract price pursuant to a provision in this Contract shall be made in one or more of the following ways:

(1) By agreement on a fixed price adjustment before commencement of the pertinent performance or as soon thereafter as practicable;

(2) By unit prices specified in the Contract or subsequently agreed upon;

(3) By the costs attributable to the event or situation covered by the provision, plus appropriate profit or fee, all as specified in the Contract or subsequently agreed upon;

(4) In such other manner as the parties may mutually agree; or

(5) In the absence of agreement between the parties, by a unilateral determination by the Agency procurement officer of the costs attributable to the event or situation covered by the provision, plus appropriate profit or fee, all as computed by the Agency procurement officer in accordance with generally accepted accounting principles and applicable sections of chapters 3-123 and 3-126, HAR.

b. Submission of cost or pricing data. The CONTRACTOR shall provide cost or pricing data for any price adjustments subject to the provisions of chapter 3-122, HAR.

22. Variation in Quantity for Definite Quantity Contracts. Upon the agreement of the STATE and the CONTRACTOR, the quantity of goods or services, or both, if a definite quantity is specified in this Contract, may be increased by a maximum of ten per cent (10%); provided the unit prices will remain the same except for any price adjustments otherwise applicable; and the Agency procurement officer makes a written determination that such an increase will either be more economical than awarding another contract or that it would not be practical to award another contract.

23. Changes in Cost-Reimbursement Contract. If this Contract is a cost-reimbursement contract, the following provisions shall apply:

a. The Agency procurement officer may at any time by written order, and without notice to the sureties, if any, make changes within the general scope of the Contract in any one or more of the following:

(1) Description of performance (Attachment 1);

(2) Time of performance (i.e., hours of the day, days of the week, etc.);

(3) Place of performance of services;

(4) Drawings, designs, or specifications when the supplies to be furnished are to be specially manufactured for the STATE in accordance with the drawings, designs, or specifications;

(5) Method of shipment or packing of supplies; or

(6) Place of delivery.

b. If any change causes an increase or decrease in the estimated cost of, or the time required for performance of, any part of the performance under this Contract, whether or not changed by the order, or otherwise affects any other terms and conditions of this Contract, the Agency procurement officer shall make an equitable adjustment in the (1) estimated cost, delivery or completion schedule, or both; (2) amount of any fixed fee; and (3) other affected terms and shall modify the Contract accordingly.

c. The CONTRACTOR must assert the CONTRACTOR'S rights to an adjustment under this provision within thirty (30) days from the day of receipt of the written order. However, if the Agency procurement officer decides that the facts justify it, the Agency procurement officer may receive and act upon a proposal submitted before final payment under the Contract.

d. Failure to agree to any adjustment shall be a dispute under paragraph 11 of this Contract. However, nothing in this provision shall excuse the CONTRACTOR from proceeding with the Contract as changed.

e. Notwithstanding the terms and conditions of subparagraphs 23a and 23b, the estimated cost of this Contract and, if this Contract is incrementally funded, the funds allotted for the performance of this Contract, shall not be increased or considered to be increased except by specific written modification of the Contract indicating the new contract estimated cost and, if this contract is incrementally funded, the new amount allotted to the contract.

24. Confidentiality of Material.

a. All material given to or made available to the CONTRACTOR by virtue of this Contract, which is identified as proprietary or confidential information, will be safeguarded by the CONTRACTOR and shall not be disclosed to any individual or organization without the prior written approval of the STATE.

b. All information, data, or other material provided by the CONTRACTOR to the STATE shall be subject to the Uniform Information Practices Act, chapter 92F, HRS.

25. Publicity. The CONTRACTOR shall not refer to the STATE, or any office, agency, or officer thereof, or any state employee, including the HOPA, the CPO, the Agency procurement officer, or to the services or goods, or both, provided under this Contract, in any of the CONTRACTOR'S brochures, advertisements, or other publicity of the CONTRACTOR. All media contacts with the CONTRACTOR about the subject matter of this Contract shall be referred to the Agency procurement officer.

26. Ownership Rights and Copyright. The STATE shall have complete ownership of all material, both finished and unfinished, which is developed, prepared, assembled, or conceived by the CONTRACTOR pursuant to this Contract, and all such material shall be considered "works made for hire." All such material shall be delivered to the STATE upon expiration or termination of this Contract. The STATE, in its sole discretion, shall have the exclusive right to copyright any product, concept, or material developed, prepared, assembled, or conceived by the CONTRACTOR pursuant to this Contract.

27. Liens and Warranties. Goods provided under this Contract shall be provided free of all liens and provided together with all applicable warranties, or with the warranties described in the Contract documents, whichever are greater.

28. Audit of Books and Records of the CONTRACTOR. The STATE may, at reasonable times and places, audit the books and records of the CONTRACTOR, prospective contractor, subcontractor, or prospective subcontractor which are related to:

a. The cost or pricing data, and

b. A state contract, including subcontracts, other than a firm fixed-price contract.

29. Cost or Pricing Data. Cost or pricing data must be submitted to the Agency procurement officer and timely certified as accurate for contracts over $100,000 unless the contract is for a multiple-term or as otherwise specified by the Agency procurement officer. Unless otherwise required by the Agency procurement officer, cost or pricing data submission is not required for contracts awarded pursuant to competitive sealed bid procedures.

If certified cost or pricing data are subsequently found to have been inaccurate, incomplete, or noncurrent as of the date stated in the certificate, the STATE is entitled to an adjustment of the contract price, including profit or fee, to exclude any significant sum by which the price, including profit or fee, was increased because of the defective data. It is presumed that overstated cost or pricing data increased the contract price in the amount of the defect plus related overhead and profit or fee. Therefore, unless there is a clear indication that the defective data was not used or relied upon, the price will be reduced in such amount.

30. Audit of Cost or Pricing Data. When cost or pricing principles are applicable, the STATE may require an audit of cost or pricing data.

31. Records Retention.

(1) Upon any termination of this Contract or as otherwise required by applicable law, CONTRACTOR shall, pursuant to chapter 487R, HRS, destroy all copies (paper or electronic form) of personal information received from the STATE.

(2) The CONTRACTOR and any subcontractors shall maintain the files, books, and records that relate to the Contract, including any personal information created or received by the CONTRACTOR on behalf of the STATE, and any cost or pricing data, for at least three (3) years after the date of final payment under the Contract. The personal information shall continue to be confidential and shall only be disclosed as permitted or required by law. After the three (3) year, or longer retention period as required by law has ended, the files, books, and records that contain personal information shall be destroyed pursuant to chapter 487R, HRS or returned to the STATE at the request of the STATE.

32. Antitrust Claims. The STATE and the CONTRACTOR recognize that in actual economic practice, overcharges resulting from antitrust violations are in fact usually borne by the purchaser. Therefore, the CONTRACTOR hereby assigns to STATE any and all claims for overcharges as to goods and materials purchased in connection with this Contract, except as to overcharges which result from violations commencing after the price is established under this Contract and which are not passed on to the STATE under an escalation clause.

33. Patented Articles. The CONTRACTOR shall defend, indemnify, and hold harmless the STATE, and its officers, employees, and agents from and against all liability, loss, damage, cost, and expense, including all attorneys fees, and all claims, suits, and demands arising out of or resulting from any claims, demands, or actions by the patent holder for infringement or other improper or unauthorized use of any patented article, patented process, or patented appliance in connection with this Contract. The CONTRACTOR shall be solely responsible for correcting or curing to the satisfaction of the STATE any such infringement or improper or unauthorized use, including, without limitation: (a) furnishing at no cost to the STATE a substitute article, process, or appliance acceptable to the STATE, (b) paying royalties or other required payments to the patent holder, (c) obtaining proper authorizations or releases from the patent holder, and (d) furnishing such security to or making such arrangements with the patent holder as may be necessary to correct or cure any such infringement or improper or unauthorized use.

34. Governing Law. The validity of this Contract and any of its terms or provisions, as well as the rights and duties of the parties to this Contract, shall be governed by the laws of the State of Hawaii. Any action at law or in equity to enforce or interpret the provisions of this Contract shall be brought in a state court of competent jurisdiction in Honolulu, Hawaii.

35. Compliance with Laws. The CONTRACTOR shall comply with all federal, state, and county laws, ordinances, codes, rules, and regulations, as the same may be amended from time to time, that in any way affect the CONTRACTOR'S performance of this Contract.

36. Conflict Between General Conditions and Procurement Rules. In the event of a conflict between the General Conditions and the procurement rules, the procurement rules in effect on the date this Contract became effective shall control and are hereby incorporated by reference.

37. Entire Contract. This Contract sets forth all of the agreements, conditions, understandings, promises, warranties, and representations between the STATE and the CONTRACTOR relative to this Contract. This Contract supersedes all prior agreements, conditions, understandings, promises, warranties, and representations, which shall have no further force or effect. There are no agreements, conditions, understandings, promises, warranties, or representations, oral or written, express or implied, between the STATE and the CONTRACTOR other than as set forth or as referred to herein.

38. Severability. In the event that any provision of this Contract is declared invalid or unenforceable by a court, such invalidity or unenforceability shall not affect the validity or enforceability of the remaining terms of this Contract.

39. Waiver. The failure of the STATE to insist upon the strict compliance with any term, provision, or condition of this Contract shall not constitute or be deemed to constitute a waiver or relinquishment of the STATE'S right to enforce the same in accordance with this Contract. The fact that the STATE specifically refers to one provision of the procurement rules or one section of the Hawaii Revised Statutes, and does not include other provisions or statutory sections in this Contract shall not constitute a waiver or relinquishment of the STATE'S rights or the CONTRACTOR'S obligations under the procurement rules or statutes.

40. Pollution Control. If during the performance of this Contract, the CONTRACTOR encounters a "release" or a "threatened release" of a reportable quantity of a "hazardous substance," "pollutant," or "contaminant" as those terms are defined in section 128D-1, HRS, the CONTRACTOR shall immediately notify the STATE and all other appropriate state, county, or federal agencies as required by law. The Contractor shall take all necessary actions, including stopping work, to avoid causing, contributing to, or making worse a release of a hazardous substance, pollutant, or contaminant, and shall promptly obey any orders the Environmental Protection Agency or the state Department of Health issues in response to the release. In the event there is an ensuing cease-work period, and the STATE determines that this Contract requires an adjustment of the time for performance, the Contract shall be modified in writing accordingly.

41. Campaign Contributions. The CONTRACTOR is hereby notified of the applicability of 11-355, HRS, which states that campaign contributions are prohibited from specified state or county government contractors during the terms of their contracts if the contractors are paid with funds appropriated by a legislative body.

42. Confidentiality of Personal Information.

a. Definitions.

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either name or data elements are not encrypted:

(1) Social security number;

(2) Driver's license number or Hawaii identification card number; or

(3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial information.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

"Technological safeguards" means the technology and the policy and procedures for use of the technology to protect and control access to personal information.

b. Confidentiality of Material.

(1) All material given to or made available to the CONTRACTOR by the STATE by virtue of this Contract which is identified as personal information, shall be safeguarded by the CONTRACTOR and shall not be disclosed without the prior written approval of the STATE.

(2) CONTRACTOR agrees not to retain, use, or disclose personal information for any purpose other than as permitted or required by this Contract.

(3) CONTRACTOR agrees to implement appropriate "technological safeguards" that are acceptable to the STATE to reduce the risk of unauthorized access to personal information.

(4) CONTRACTOR shall report to the STATE in a prompt and complete manner any security breaches involving personal information.

(5) CONTRACTOR agrees to mitigate, to the extent practicable, any harmful effect that is known to CONTRACTOR because of a use or disclosure of personal information by CONTRACTOR in violation of the requirements of this paragraph.

(6) CONTRACTOR shall complete and retain a log of all disclosures made of personal information received from the STATE, or personal information created or received by CONTRACTOR on behalf of the STATE.

c. Security Awareness Training and Confidentiality Agreements.

(1) CONTRACTOR certifies that all of its employees who will have access to the personal information have completed training on security awareness topics relating to protecting personal information.

(2) CONTRACTOR certifies that confidentiality agreements have been signed by all of its employees who will have access to the personal information acknowledging that:

(A) The personal information collected, used, or maintained by the CONTRACTOR will be treated as confidential;

(B) Access to the personal information will be allowed only as necessary to perform the Contract; and

(C) Use of the personal information will be restricted to uses consistent with the services subject to this Contract.

d. Termination for Cause. In addition to any other remedies provided for by this Contract, if the STATE learns of a material breach by CONTRACTOR of this paragraph by CONTRACTOR, the STATE may at its sole discretion:

(1) Provide an opportunity for the CONTRACTOR to cure the breach or end the violation; or

(2) Immediately terminate this Contract.

In either instance, the CONTRACTOR and the STATE shall follow chapter 487N, HRS, with respect to notification of a security breach of personal information.

e. Records Retention.

(1) Upon any termination of this Contract or as otherwise required by applicable law, CONTRACTOR shall, pursuant to chapter 487R, HRS, destroy all copies (paper or electronic form) of personal information received from the STATE.

(2) The CONTRACTOR and any subcontractors shall maintain the files, books, and records that relate to the Contract, including any personal information created or received by the CONTRACTOR on behalf of the STATE, and any cost or pricing data, for at least three (3) years after the date of final payment under the Contract. The personal information shall continue to be confidential and shall only be disclosed as permitted or required by law. After the three (3) year, or longer retention period as required by law has ended, the files, books, and records that contain personal information shall be destroyed pursuant to chapter 487R, HRS or returned to the STATE at the request of the STATE.

ADDITIONAL GENERAL CONDITIONS FOR GOODS AND SERVICES CONTRACTS

INTENT OF CONTRACT:

The intent of the contract is to provide for the service, complete in every detail, of the work described. The Contractor shall furnish all labor, materials, equipment, tools, transportation and supplies required to complete the work in accordance with the specifications and terms of the contract.

INTERPRETATION OF SPECIFICATIONS:

Should it appear that the work to be done or any of the matters relative thereto are not sufficiently detailed or explained in the specifications, the Contractor shall apply to the Contracting Officer for such further explanations as may be necessary and shall conform to same as part of the contract, so far as may be consistent with the original specifications; and in the event of any doubt or questions arising respecting the true meaning of the specifications, reference shall be made to the Contracting Officer whose decision thereon shall be final.

LIABILITY INSURANCE:

The Contractor shall not commence any work until it obtains, at its own expense, all required liability insurance. Such insurance must have the approval of the State as to limit form and amount and must be maintained with a company acceptable to the State. Such insurance must be maintained for the full period of the contract and shall provide protection from claims arising out of or resulting from the Contractor's operations under the Contract itself Subcontractor or by anyone directly or indirectly employed by any of them or by anyone for whose acts any of them may be liable.

The contractor shall take out and maintain during the life of this contract broad form public liability (Bodily Injury) and broad form property damage liability insurance in a combined single limit not less than $1,000,000 and not less than $2,000,000 in the aggregate to protect such contractor and all his subcontractors from claims for damages for personal injury, accidental death and property damage which may arise from operations under this contract, whether such operations be by himself or anyone directly or indirectly employed by either of them.

The insurance described herein will be maintained by the Contractor for the full period of the Contract and in no event will be terminated or otherwise allowed to lapse prior to final acceptance of the work by the State.

A certificate of insurance acceptable to the State shall be filed with the State prior to commencement of the work. Such certificate shall contain a provision that coverage afforded under the policy will not be canceled or changes until at least thirty days written notice has been given to the State by registered mail at the address denominated for the State in the Contract for

official communications to it should any policy be canceled before final acceptance by the State, and the Contractor fails to immediately procure replacement insurance as specified, the State reserves the right to procure such insurance and to deduct the cost thereof from any sum due the Contractor.

LAWS TO BE OBSERVED:

The Contractor at all times shall observe and comply with all Federal, State and local laws or ordinances, rules and regulations which in any manner affect those engaged or employed in the work, the materials used in the work, and the conduct of the work. The Contractor shall also comply with all such orders and decrees of bodies or tribunals having any jurisdiction or authority over the work. Any reference to such laws, ordinances, rules and regulations shall include any amendments thereto.

The Contractor shall protect and indemnify the State and its Departments and Agencies and all their officers, representatives, employees or agents against any claim or liability arising from or based on the violation of any such laws, ordinances, rules and regulations, orders and decrees, whether such violation is committed by the Contractor or his subcontractor or the employee of either or both. If any discrepancy or inconsistency is discovered in the contract for the work in relation to any such laws, ordinances, rules and regulations, orders or decrees, the Contractor shall forthwith report the same to the State of Hawaii, Department of Defense, Engineer in writing.

Attention is directed to the Hawaii Employment Relations Act, Chapter 377, HRS; Hawaii Employment Security Law, Chapter 383, HRS; Wage and Hour Law, Chapter 387, HRS; Payment of Wages, Chapter 388, HRS; and Worker's Compensation Law, Chapter 386, HRS.

Workers' Compensation - The Contractor shall, in accordance with Sections 386-121 to 386-129 Hawaii Revised Statutes, inclusive, take out adequate worker's compensation insurance for all of his employees who will be engaged in work at the site of the project.

PERMITS AND LICENSES:

The Contractor shall procure all permits and licenses, pay all charges and fees and give all notices necessary and incident to the due and lawful prosecution of the work.

CHARACTER OF WORKERS OR EQUIPMENT:

A. Character and Proficiency of Workers - All workers must have sufficient skill and experience to perform the work assigned to them and in the operation of the equipment.

Any worker employed on the project by the Contractor who, in the opinion of the Engineer or his authorized representative, is not careful and competent, does not perform his work in a proper and skillful manner or is disrespectful, intemperate, disorderly or neglects or refuses to comply with directions given, or is otherwise objectionable shall, at the written request of the

Engineer, be removed forthwith by the Contractor employing such worker and shall not be employed again in any portion of the work without the written consent of the Engineer. Should the Contractor continue to employ, or again employ such person(s) on the project, the Engineer will withhold all estimates which are or may become due, or the Engineer will suspend the work until such orders are complied with.

B. Insufficient Workers - In the event that the Engineer, in his judgment, finds the condition whereby insufficient workers are present to accomplish the work and no corrective action is taken by the Contractor after being informed, the Engineer reserves the right to terminate the contract.

C. Equipment Requirements - All equipment furnished by the Contractor and used shall be of such size and of such mechanical condition that the work can be prosecuted in an acceptable manner.

RIGHT TO AUDIT RECORDS

Pursuant to Section 103D-317 HRS the State, at reasonable times and places, may audit the books and records relating to the contractor's cost or pricing data. The books and records shall be maintained for a period of three years from the date of final payment under the contract, unless another period is otherwise authorized in writing.

Additionally, Sections 231-7, 235-108, 237-39 and other HRS chapters through reference, authorizes the Department of Taxation to audit all taxpayers conducting business within the State. Contractors must make available to the Department of Taxation all books and records necessary to verify compliance with the tax laws.

The following sections of the Hawaii Administrative Rules, Chapter 3-125 are amended as shown below.

CHANGE ORDERS TO GOODS AND SERVICES CONTRACTS – HAR 3-125-2

1. Change clause. By written order, at any time, and without notice to any surety, the procurement officer may, unilaterally, order of the contractor:

   a. Changes in the work within the scope of the contract; and
   b. Changes in the time of performance of the contract that do not alter the scope of the contract work.

2. Adjustments of price or time for performance. If any change order increases or decreases the contractor's cost of, or the time required for, performance of any part of the work under this contract, an adjustment shall be made and the contract modified in writing accordingly. Any adjustment in contract price made pursuant to this clause shall be determined, where applicable, in accordance with the price adjustment clause of this contract or as negotiated. Failure of the parties to agree to an adjustment shall not excuse the contractor from

proceeding with the contract as changed, provided that the procurement officer promptly and duly makes the provisional adjustments in payment or time for the direct costs of the work as the State deems reasonable. The right of the contractor to dispute the contract price or time required for performance or both shall not be waived by its performing the work, provided however, that it follows the written notice requirements for disputes and claims established by the contract or these rules.

3. Time Period for Claim. Within 10 days after receipt of a written change order, unless the period is extended by the procurement officer in writing, the contractor shall respond with a claim for an adjustment. The requirement for a timely written response cannot be waived and shall be a condition precedent to the assertion of a claim.

4. Claim barred after final payment. No claim by the contractor for an adjustment hereunder shall be allowed if written response is not given prior to final payment under this contract.

5. Claims not barred. In the absence of a change order, nothing in this clause shall be deemed to restrict the contractor's right to pursue a claim under the contract or for breach of contract.

MODIFICATIONS TO GOODS AND SERVICES CONTRACTS – HAR 3-125-3

1. Contract Modification. By a written order, at any time, and without notice to any surety, the procurement officer, subject to mutual agreement of the parties to the contract and all appropriate adjustments, may make modifications within the general scope of this contract to include any one or more of the following:

   a. Drawings, designs, or specifications, for the goods to be furnished;
   b. Method of shipment or packing;
   c. Place of delivery;
   d. Description of services to be performed;
   e. Time of performance (i.e., hours of the day, days of the week, etc.);
   f. Place of performance of the services; or
   g. Other provisions of the contract accomplished by mutual action of the parties to the contract.

2. Adjustments of price or time for performance. If any modification increases or decreases the contractor's cost of, or the time required for, performance of any part of the work under this contract, an adjustment shall be made and the contract modified in writing accordingly. Any adjustment in contract price made pursuant to this clause shall be determined, where applicable, in accordance with the price adjustment clause of this contract or as negotiated.

3. Claim barred after final payment. No claim by the contractor for an adjustment hereunder shall be allowed if written agreement of modification is not made prior to final payment under this contract.

4. Claims not barred. In the absence of a contract modification, nothing in this clause shall be deemed to restrict the contractor's right to pursue a claim under the contract or for a breach of contract.

PRICE ADJUSTMENT FOR GOODS AND SERVICES CONTRACTS – HAR 3-125-12

1. Price adjustment. Any adjustment in contract price pursuant to a clause in this contract shall be made in one or more of the following ways;

a. By agreement on a fixed price adjustment before commencement of the pertinent performance or as soon thereafter as practicable;
b. By unit prices specified in the contract or subsequently agree upon;
c. By the costs attributable to the event or situation covered by the clause, plus appropriate profit or fee, all as specified in the contract or subsequently agreed upon;
d. In such other manner as the parties may mutually agree; or
e. In the absence of agreement between the parties, by a unilateral determination by the procurement officer of the costs attributable to the event or situation covered by the clause, plus appropriate profit or fee, all as computed by the procurement officer in accordance with generally accepted accounting principles and applicable sections of chapters 3-122 and 3-126, Hawaii Administrative Rules.

2. Submission of cost or pricing data. The contractor shall provide cost or pricing data for any price adjustments subject to the provision of subchapter 15, chapter 3, 122, Hawaii Administrative Rules.

PROMPT PAYMENT BY CONTRACTORS TO SUBCONTRACTORS – HAR 3-125-23

1. Prompt payment clause. Any money, other than retainage, paid to a contractor shall be dispersed to subcontractors within ten days after receipt of the money in accordance with the terms of the subcontract; provided that the subcontractor has met all the terms and conditions of the subcontract and there are no bona fide disputes; and, upon final payment to the contractor, full payment to the subcontractor, including retainage, shall be made within ten days after receipt of the money; provided that there are no bona fide disputes over the subcontractor's performance under the subcontract.

SECTION 40 OF THE GENERAL CONDITIONS HAS BEEN CHANGED TO READ AS:

40. Environmental Compliance

A. Pollution Control - If during the performance of this Contract, the CONTRACTOR encounters a "release" or a "threatened release" of a reportable quantity of a "hazardous substance," "pollutant," or "contaminant" as those terms are defined in section 128D-1, HRS or any other environmental law, regulation, or permit requirement, the CONTRACTOR shall immediately notify the STATE and all other appropriate state, county, or federal agencies as

required by law. The Contractor shall take all necessary actions, including stopping work, to avoid causing, contributing to, or making worse a release of a hazardous substance, pollutant, or contaminant, and shall promptly obey any orders the Environmental Protection Agency or the state Department of Health issues in response to the release. In the event there is an ensuing cease-work period, and the STATE determines that this Contract requires an adjustment of the time for performance, the Contract shall be modified in writing accordingly.

B. Non-Compliance Notifications - The Project Manager will notify the Contractor in writing within 3 business days of any observed noncompliance with federal, state, or local environmental laws or regulations, permits, and other elements of the Contractor's Environmental Protection Plan. After receipt of such notice, CONTRACTOR will inform the Project Manager of the proposed corrective action within 3 business days. After acceptance of the proposed action by the Project Manager, the Contractor shall take such action within 5 business days. The Contracting Officer may issue an order of suspension of all or part of the work until satisfactory corrective action has been taken. A suspension, delay, or interruption of work due to the fault or negligence of the Contractor, in whole or in part, will not justify an adjustment to the contract for time extensions or equitable adjustments. In addition to a suspension of work, the Contracting Officer or Project Manager may exercise any additional remedy authorized by law or the contract. Failure to comply with this requirement within a time period specified by the Project manager constitutes a material breach of the contract.

OVERVIEW OF THE RFP PROCESS

1. The RFP is issued pursuant to Subchapter 6 of HAR Chapter 3-122, implementing HRS §103D-303.

2. The procurement process begins with the issuance of the RFP and the formal response to any written questions or inquiries regarding the RFP. Changes to the RFP will be made only by Addendum.

3. Proposals shall be received on HePS. The register of proposals and Offerors' proposals shall be open to public inspection after posting of the award.

   All proposals and other material submitted by Offerors become the property of the State and may be returned only at the State's option.

4. The Procurement Officer, or an evaluation committee approved by the Procurement Officer, shall evaluate the proposals in accordance with the evaluation criteria in Section Four.

5. Proposals may be accepted on evaluation without discussion. However, if deemed necessary, prior to entering into discussions, a "priority list" of responsible Offerors submitting acceptable and potentially acceptable proposals shall be generated. The priority list may be limited to a minimum of three responsible Offerors who submitted the highest-ranked proposals. The objective of these discussions is to clarify issues regarding the Offeror's proposal before the BAFO is tendered.

6. If during discussions there is a need for any substantial clarification or change in the RFP, the RFP shall be amended by an addendum to incorporate such clarification or change. Addenda to the RFP shall be distributed only to priority listed Offerors who submit acceptable or potentially acceptable proposals.

7. Following any discussions, Priority Listed Offerors will be invited to submit their BAFO, if required. The Procurement Officer or an evaluation committee reserves the right to have additional rounds of discussions with the top three (3) Priority Listed Offerors prior to the submission of the BAFO.

8. The date and time for Offerors to submit their BAFO, if any, is indicated in Section 1.4, RFP Schedule and Significant Dates. If Offeror does not submit a notice of withdrawal or a BAFO, the Offeror's immediate previous offer shall be construed as its BAFO.

9. After receipt and evaluation of the BAFOs in accordance with the evaluation criteria in Section Four, the Procurement Officer or an evaluation committee will make its recommendation. The Procurement Officer will award the contract to the Offeror whose proposal is determined to be the most advantageous to the State taking into consideration price and the evaluation factors set forth in Section Four.

10. The contents of any proposal shall not be disclosed during the review, evaluation, or discussion. Once award notice is posted, all proposals, successful and unsuccessful, become available for public inspection. Those sections that the Offeror and the State agree are confidential and/or proprietary should be identified by the Offerors and shall be excluded from access.

11. The Procurement Officer or an evaluation committee reserves the right to determine what is in the best interest of the State for purposes of reviewing and evaluating proposals submitted in response to the RFP. The Procurement Officer or an evaluation committee will conduct a comprehensive, fair and impartial evaluation of proposals received in response to the RFP.

12. The RFP, any addenda issued, and the successful Offeror's proposal shall become a part of the contract. All proposals shall become the property of the State of Hawai'i.

Presented by the
State of Hawai'i Office
of Homeland Security

dod.hawaii.gov/ohs

HAWAI'I
TARGETED VIOLENCE PREVENTION STRATEGY

2022

THIS PAGE
INTENTIONALLY
LEFT BLANK

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Targeted violence involves acts dangerous to human life that are in violation of the criminal laws of the United States or of any State and that involve a degree of planning and involve a pre-identified target including individual(s) based on actual or perceived identity traits or group affiliation or property based on actual or perceived identity traits or group affiliation; and appears intended to intimidate, coerce, or otherwise impact a broader population beyond the target(s) of the immediate act; or generate publicity for the perpetrator or his or her grievances; and occurs within the territorial jurisdiction of the United States; and excludes acts of interpersonal violence, street or gang-related crimes, or financially motivated crimes.

Ideologically inspired violence can disrupt communities and impact the health, safety, and well-being of children, families, and other vulnerable populations, social services, education, public health, and civil rights officials.

Preventing targeted violence requires a coalition of stakeholders that extends beyond law enforcement. The intersectional nature of the threat necessitates a multidisciplinary approach to identify and address the root cause of violence to mitigate it from spreading. The principles of public health and a "Whole of Community" approach provide a useful framework for addressing this issue.

A multidisciplinary effort is not enough, however. The approach must be supported by enabling processes that allow for multidirectional communication and collaboration between the various stakeholders and government entities, underpinned by appropriate resourcing and governance.

The Office of Homeland Security (OHS) plays a statutory role in ensuring the safety and wellbeing of all who live in the state. Protecting Hawaii's residents and visitors from targeted violence is one of its most important duties. OHS has unique convening capabilities that can be leveraged to develop broad stakeholder buy-in for a statewide vision on Targeted Violence Prevention (TVP).

INTRODUCTION

Targeted violence is intentional, instrumental, and proactive violence, as opposed to impulsive, emotional, and reactive violence. It is rarely, if ever, sudden, or spontaneous. In fact, by definition, targeted violence is premeditated and planned, even if done over a relatively short period of time. Targeted violence is the result of an understandable, and often discernible, process of thinking and behavior. It arises from the dynamic interactions between an identifiable person of concern, their intended target, their current situation or life circumstances, and the operational setting for their intended violence[1]. Targeted violence is a highly individualized crime, driven by highly individualized, variable, and often multiple motivations, which sometimes remain undiscovered or undetermined, but generally include the intent to intimidate or coerce or generate publicity about the perpetrator's grievance[2].

The U.S. Intelligence Community assessed that "domestic violent extremists who are motivated by a range of ideologies and galvanized by recent political and societal events in the United States pose an elevated threat" in 2021. Terrorist attacks have changed in recent years. Whereas terrorist organizations used to be responsible for most terrorism incidents, recently, within the U.S., lone offenders or small cells are more likely to carry out violent attacks.

Now that lone offenders are committing more attacks than terrorist organizations in the U.S., targeted violence does not depend on large groups training, planning, or completing attacks together. Instead, lone offenders train, practice, and complete their attacks based on the tactics, techniques, and procedures (TTPs) of previous offenders. They research prior attacks and then emulate them, from manifestos to iconography to publicizing their acts of mass violence. Likewise, lone offenders do not need large quantities of weapons because lone offenders pick "soft targets" – places such as shopping centers, schools, or houses of worship that do not have strong physical fortifications.

While addressing targeted violence is a pressing national challenge, Hawai'i is not immune to the threat. Examples of planned, completed, or emerging threats of targeted violence in Hawai'i include:

While addressing targeted violence is a pressing national challenge, it is not unique to Hawai'i. Examples of planned, completed, or emerging threats of targeted violence in Hawai'i include:

- **1999** Xerox shooting *(workplace violence)*
- **2019** Pearl Harbor shipyard shooting *(workplace violence, military target)*
- **2019 through 2022** Threats of mass violence at schools *(soft target)*
- **2021** Diamond Head shooting/arson *(domestic and anti-government violence)*
- **2022** Increase in threats to Hawai'i judges *(anti-government violence)*

Hawai'i is the "cultural melting pot" of the Pacific. It is notable in many ways: by geographical separation and location in the Pacific Ocean (apart from the rest of the 48 contiguous states);

as an island chain in which different communities are located on separate islands; and as a designated majority-minority state. This places Hawai'i in a unique position to address an issue that all states are working hard to address: the prevention of targeted violence.

The challenges we face are also noteworthy. Our geographical location allows our community members to create distinctions between what happens in the continental United States (CONUS), and what happens (or does not happen) in our islands. Our distance from many of the tragic events that have recently occurred in the CONUS, allows us to wrongfully think 'what happens there, could never happen here.' However, those events serve as a reminder to our communities that we are not immune from tragedies; they can happen anytime and anywhere.

Hawai'i is particularly vulnerable to targeted violence due to its abundance of soft targets related to a dominant tourism industry, its strategic Asia-Pacific location and U.S. military-related infrastructure, and the fact that perpetrators who seek to target victims based on identity or group membership can find almost any target they are looking for among Hawaii's diverse population and cultures.

Since 2017, when Threat Team Oahu (TTO) was created (and since transitioned to Threat Team Hawai'i (TTH) in 2021), Hawai'i has been working hard to collaborate and build Behavior Intervention/Threat Assessment and Management (BI/TAM) strategies that support our diverse island residents and the communities they serve. These synergistic efforts lay the foundation for Hawaii's "Whole of Community" approach.

When community organizations can recognize and appropriately respond to concerning behavior (which may include threatening behavior or behavior leading to targeted violence), the possibility of averting targeted violence increases[3]. Increased community capability and awareness in identifying, assessing, intervening, and managing those behaviors which cause concern, is a necessary first step in ensuring the health and safety of our communities and the foundation which the "Whole of Community" approach is based upon.

VISION

The State of Hawai'i recognizes an urgent need to commit additional state resources to address the persistent threat of targeted violence, especially mass targeted violence, to Hawaii's public safety. Specifically, the state government envisions the need for a statewide, whole-of-community strategy that effectively counters all forms of targeted violence, across all social domains. The Hawai'i Office of Homeland Security leads the effort to develop and implement a comprehensive, community based Targeted Violence Prevention Strategy, grounded in modern, operational methodologies and best practices.

The initial goal to achieving the state vision is establishment of this comprehensive statewide **TVP Strategy** (supported by a subsequent Implementation Plan) **(Goal 1)**:

- rooted in local needs, risk, challenges, and cultural contexts;
- developed with insights from different stakeholders;
- incorporating a multi-phase (primordial, primary, secondary, and tertiary) approach to prevent targeted violence;
- reflecting collaboration across relevant agencies and organizations; and
- containing mechanisms for learning, continuous improvement, and outcome evaluation.

MISSION

To strengthen public safety across Hawai'i by mitigating or preventing all forms of targeted violence, including mass targeted violence, across all social domains.

PILLARS

1

Communicating and Collaborating

Communication and collaboration provide key opportunities to engage and inform the community about the prospect of targeted violence, how to identify it, reduce its likelihood, and direct attention and resources to build capacity that addresses it before it happens. There are several goals (with supporting objectives) within this pillar that this strategy encompasses:

- Reduce and mitigate community and individual risk factors **(Goal 5)**
  - Support development/adaptation of evidence-based efforts that address community-level risk factors
  - Support development/adaptation of evidence-based efforts that address individual-level risk factors
- Educate community on what targeted violence is and what are effective targeted violence prevention approaches **(Goal 6)**
  - Educate public about radicalization to violence, threats of targeted violence, ways to intervene, and other TVP-relevant topics
  - Increase public willingness, and knowledge of how, to seek help for individuals at risk
- Ensure BI/TATs operate effectively throughout the state **(Goal 7)**
  - Ensure public knows about BI/TATs and how to refer individuals deemed at risk
- Foster community resilience in the aftermath of a targeted violence event and prevent cycles of violence **(Goal 8)**
  - Develop clear and effective action plans for how implementation partners and other stakeholders should engage to foster community resilience and prevent cycles of violence in the aftermath of a targeted violence event
  - Ensure culturally sensitive tailored services are available for individuals, families, and communities
  - Disseminate information to the public about the availability of support
- Facilitate rehabilitation of individuals who previously engaged in targeted violence and/or who became at-risk for targeted violence while in correctional facilities **(Goal 9)**
  - Support in-prison disengagement programs
  - Support provision of wrap-around aftercare/re-entry services
  - Support implementation of disengagement programs for individuals who previously engaged in targeted violence, with or without recent justice system involvement
  - Prepare communities to receive individuals who previously engaged in targeted violence upon their release
- Sustain conducive environment **(Goal 10)**
  - Sustain public awareness and support

2

Behavior Intervention/Threat Assessment Management Teams

Behavior Intervention/Threat Assessment Management (BI/TAM) Teams (BI/TATs), at both the institutional and county levels, are operational teams that implement multidisciplinary approaches to prevent targeted violence and identify needs within their communities.

While there are important ongoing efforts to create, train, and implement BI/TATs, particularly within state educational (K-12 and higher-ed) institutions, statewide institutionalization of an operationally effective, multi-domain, coordinated network of implementation partners is the direction this strategy aims to take. **(Goals 2, 4, 7)**

Objectives that support these goals include:

- Ensure BI/TATs operate effectively throughout the state
  - Establish case management system that is comprehensive, user-friendly, safe, and capable of running anonymized reports to facilitate BI/TATs' work
  - Establish secure, effective, and diversified referral system
- Secure participation of key federal, state, and local governmental agencies and non-governmental organizations as strategy implementation partners
- Outline areas of responsibility for each implementation partner within the network
- Ensure strong in-network collaboration and communication strategies
- Provide the guidance and support needed for counties, schools, businesses, and all other interested entities to create and operate BI/TATs
- Ensure that each state county is covered by BI/TATs
- Ensure sufficient locally rooted and well-resourced aftercare services support BI/TATS
- BI/TATS are well-equipped to conduct their work and can collaborate effectively
- BI/TATS are monitored and evaluated for performance effectiveness

3

Resourcing and Governance

The Hawai'i TVP Program is housed within the Hawai'i Office of Homeland Security (OHS). Through pre-established information sharing networks and support mechanisms, the OHS provides a management structure that enables administration of the Hawai'i TVP Program and ensures implementation partners have the necessary information, resources, and guidance to conduct their prevention work. OHS facilitates the Hawai'i TVP Program State Team, which is a multidisciplinary administrative team that identifies unique approaches and promising practices to prevent targeted violence and implements them statewide. The Hawai'i TVP Program State Team liaises across disciplines and provides standardized training and events to connect and educate prevention partners and community members.

The Hawai'i TVP Program provides a variety of resources, including:

- training and events,
- program implementation and evaluation support,
- standardized forms and templates,
- communication and referral hub for network of violence prevention practitioners,
- analytic support, and
- support and consultation for complex cases.

Implementation partners and stakeholders envisioned for this TVP Strategy include:

- Public Safety
  - Department of Law Enforcement
    - Office of Homeland Security
      - Hawai'i State Fusion Center
  - Department of the Attorney General
  - Department of Corrections and Rehabilitation
  - Hawai'i State Judiciary
  - County Police Departments
- Health And Human Services
  - Department of Health
  - Department of Human Services
  - Office of Veterans' Services
  - Hawai'i Civil Rights Commission

- Education
  - Department of Education
  - Hawai'i State Charter School Commission
  - University of Hawai'i system
- Emergency Management
  - Hawai'i Emergency Management Agency
  - County Emergency Management/Civil Defense
- Non-Government
  - Private K-12 and post-secondary education institutions
  - Private hospitals and healthcare clinics
  - Mental wellness providers
  - Direct social service providers (e.g., housing, food security, victim support services, immigrant and refugee support, substance abuse rehabilitation programs, suicide prevention and other crisis intervention services)
  - Advocacy and access organizations (e.g. legal services, disability and vocational rehabilitative services, language access)
  - Community groups (e.g., neighborhood groups, communities of faith, youth groups, other clubs and organizations)

While the HSFC and state threat assessment efforts through Threat Team Hawai'i have been ongoing for several years, the establishment of this TVP Strategy adds significant resourcing and governance focus and structure to those efforts as they relate to TVP. Resourcing and governance are key to enabling this strategy to succeed, providing the less-visible structural elements that will underpin the strategy's two other pillars. Cross-cutting goals and their objectives include **(Goals 4, 7, 10)**:

- Build capacity among key stakeholders and agencies
  - Secure funding to provide TVP programming implementation and evaluation support
  - Facilitate TVP programming implementation and evaluation efforts
- Establish unified systems and provide technologies that will facilitate monitoring and evaluation
- Ensure BI/TATs operate effectively throughout the state
  - BI/TATS are monitored and evaluated for performance effectiveness
- Sustain conducive environment
  - Sustain funding

Statewide Information Sharing

The Hawai'i State Fusion Center (HSFC) is Hawaii's hub for statewide information and intelligence sharing, as well as data analysis. As they apply to targeted violence prevention, the HSFC efforts supports use of evidence-informed methods to accomplish the goals and objectives outlined in this strategy.

This includes the following best practices for data collection and analysis:

- Use of multiple qualitative and quantitative data sources, including
  - **Law enforcement data** to learn **WHERE** violence happens, **WHO** is involved in violence, **WHAT** type of violence is occurring, and **WHEN** violence most frequently occurs.
  - **Public health data** to learn **WHO** is victimized, **WHEN** victimization occurs, and **WHAT** type of victimization is most frequent.
  - **Community organization data** to learn **WHO** is receiving services for involvement in violence, **WHERE** community residents do not feel safe, **WHY** violence is occurring in certain places, **WHAT** are the community's assets and needs, **WHO** are trusted leaders in the community, and **WHAT** are the underlying issues that cause violence.
  - **Landscape analysis** to learn about the historical, current, and proposed policies, strategies, and systems impacting the community and community violence.
- Leveraging HSFC's analytical capabilities to inform training efforts and resource allocation.
- Checks for biases in data sources to mitigate their influence; consulting with research or technical assistance partners as necessary.
- Identifying community policies, community comprehensive plans, and local assets and noting existing strengths that can be built upon for TVP efforts, in addition to identifying any needs/gaps.
- Examining local capacity for systems-led and community-based leadership of TVP.

Professional Education, Training, and Consultation

Professional education, training, and consultation support must be strategic and meaningful to ensure program stability and its capacity for success. This often requires both financial and technical assistance to target development of specific capabilities needed to implement this TVP strategy. Whether by facilitating or actual provision of, the availability of these ongoing enabling activities can incentivize the construction of an effective TVP Program. Facilitation of this assistance can also mean steering elements of this TVP Program to Federal programs like the Department of Homeland Security's Center for Prevention Programs and Partnerships (CP3) Targeted Violence and Terrorism Prevention grant program who can provide promising practices, as well as technical assistance.

The overarching goals and their supporting objectives here include:

- Build capacity among key stakeholders and agencies **(Goal 4)**
  - Equip implementation partners with knowledge relevant to targeted violence and best practices in prevention and intervention for different areas of service provision
- Support professional development, learning, and improvement **(Goal 11)**
  - Provide the implementation partners with available up-to-date research evidence and best practices for effective TVP efforts
  - Support professional development of the implementation partners and relevant stakeholders
  - Monitor the strategy implementation
  - Facilitate ongoing learning and improvement activities

3.2

Privacy, Civil Rights, and Civil Liberties

The HSFC is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to prevent targeted violence by analyzing data from a variety of sources. Today's increased security needs not only dictate enhanced information sharing but also highlight the need to balance the sharing of information with the rights of persons in the United States. Ethical and legal obligations compel personnel, authorized users, and participating entities to protect constitutional rights, including privacy and other civil liberties, and civil rights throughout the information sharing process. To accomplish this, appropriate privacy, civil rights, and civil liberties protection policies must be in place.

A privacy, civil rights, and civil liberties (P/CRCL) policy is a written, published statement that articulates HSFC's position on how it handles the personally identifiable information (PII) and other personal, sensitive information it seeks, receives, or uses in the normal course of business. Civil rights and civil liberties protections are clearly expressed in the HSFC P/CRCL policy. The purpose of a P/CRCL policy is to articulate within the HSFC, to external agencies that access and share information with the center, to other entities, and publicly that the center will adhere to legal requirements and policy and procedural provisions that enable gathering and sharing of information to occur in a manner that protects constitutional rights, including personal privacy and other civil liberties, and civil rights.

In addition, TVP programming will protect P/CRCL by training stakeholders in the applicable law and supporting program development that reflects the values inherent in the law.

3.3

Legislative Framework

As a legislatively assigned office, the Office of Homeland Security's (OHS') responsibilities are defined in the Hawai'i Revised Statutes (HRS). OHS is established by Act 175, passed by the 2013 State legislature, codified in HRS § 128A[4], and added to in 2015 with HRS § 128B[5]. Updates to HRS § 128B – adjusting the current language that connotes a singular position to that which describes a statewide program – were introduced in the 2022 Legislative Session and their intent are generally reflected in the below.

HRS § 128A established OHS and its responsibilities, while HRS § 128B established additional powers and duties relative to cybersecurity.

HRS § 128A's purpose is to "provide for all homeland security functions of this State and its counties" through the following:

- Provide for homeland security by the State and to authorize the creation of organizations for homeland security in the counties of the State; and
- In coordination with county agencies, other state and federal agencies, and the private sector, provide programs to educate and train publicly and privately employed workers and the general public to be prepared for potential attacks.

HRS § 128A provides Office of Homeland Security leadership the discretionary authority to:

- Prepare comprehensive plans and programs for homeland security and homeland defense; provided that these plans and programs shall be integrated and coordinated with the plans of the counties and the federal government to the fullest possible extent;
- Make studies and surveys of the vulnerabilities of critical infrastructure and essential resources in this State as may be necessary, and participate in planning for their protection;
- Develop and maintain a list of critical infrastructure, coordinating the list with the counties of the State, other state agencies, federal agencies (including the Departments of Defense and Homeland Security), the private sector, and other agencies and organizations as necessary;
- Develop and maintain a capability to process security-clearance applications for civilian workers of the state and county governments;
- Foster coordination on security matters with all nations of the Pacific region to the extent permitted under federal law, including but not limited to coordinating planning efforts, as appropriate; sponsoring discussions and seminars; and hosting periodic international conferences; and
- Solicit and manage funding, including but not limited to grants from the federal government, funds from other divisions in the department of defense and other state agencies, and funds to provide personnel support to the Office of Homeland Security.

HRS § 128B added to the Office of Homeland Security authorities, requiring partnering with specific entities and development of the requirements for the components of a cybersecurity program, such as 'improving cyber resiliency within the State and its critical infrastructure network by using existing resources within the State.'

Building on the above legislative foundation is critical to establishing the Hawai'i TVP Program as envisioned by this Strategy. It is also a process, by which this strategy intends to meet the twin goals of first securing a conducive environment for strategy implementation and then sustaining that environment. **(Goals 3, 10)** The objectives underpinning these goals are first, ensuring political will and community buy-in and secondly, sustaining both.

At the time of development of this TVP Strategy, two significant legislative proposals are in development for a future legislative session. One encompasses formal establishment of the HSFC. The second mirrors the vision and scope of this strategy. The following descriptions reflect the current state of conceptual language of those proposals, the specific content of legislation being subject to change during the legislative process.

Hawai'i State Fusion Center:

The proposal currently being shaped through the development of this TVP Strategy and would establish in statute the HSFC under the Office of Homeland Security as described in HRS § 128A. The basic legislative proposal will be considered for re-proposal to include requirements for the HSFC to:

- Be continually staffed to monitor all crimes and hazards and shall be the focal point for sharing local, national, and international information and context with the national level intelligence community;
- Collaborate among all levels of government to receive, analyze, and disseminate threat-related information in coordination with multi-disciplinary partners; and
- Establish a joint integration center to:
  - Integrate information technology, cybersecurity, and cybercrime prevention, and cyber and analytic capabilities, and to improve situational awareness related to critical infrastructure or key resources protection of lifelines;
  - Coordinate with local, state, and federal agencies for asset response activities to include:
    - Furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;
    - Identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities;
    - Assessing potential risks to the State or region, including potential cascading effects, and developing courses of action to mitigate these risks;
    - Facilitating information sharing and operational coordination to respond to threats; and
    - Providing guidance as to how best to utilize federal resources and capabilities in a timely, effective manner to speed recovery; and
- Provide intelligence support and related activities, facilitate the building of situational threat awareness and sharing of related intelligence, including the integrated analysis of threat trends and events, the identification of knowledge gaps, and the ability to degrade or mitigate adversary threat capabilities.

Targeted Violence Prevention:

The current proposal being crafted was also matured through the development of this TVP Strategy and will be considered for proposal in future legislative sessions, focusing on:

- formally establishing a targeted violence prevention program within the state office of homeland security;
- requiring establishment of behavioral intervention/threat assessment management teams in K-12 and higher educational institutions, public and private
- mandating reporting, referral, and collaboration mechanisms; and
- authorizing program resourcing and governance.

APPENDICES

Appendix A – References

Antiterrorism Act, 18 U.S.C. § 2331 (1990).

Bureau of Justice Assistance; *Community Based Violence Intervention and Prevention Initiative Implementation Checklist* (April, 2022). Accessed August 18, 2022 at: https://bja.ojp.gov/program/community-violence-intervention/implementation-checklist

Congressional Research Service; *Sifting Domestic Terrorism from Domestic Violent Extremism and Hate Crime* (June 1, 2022). Accessed June 27, 2022 at: https://sgp.fas.org/crs/terror/IN10299.pdf

Department of Homeland Security, Center for Prevention Programs and Partnerships (CP3). Accessed June 27, 2022 at: https://www.dhs.gov/CP3

Department of Homeland Security, National Threat Evaluation and Reporting (NTER) Office. Accessed June 27, 2022 at: https://www.dhs.gov/nter

Federal Bureau of Investigation, Behavioral Analysis Unit (BAU), Behavioral Threat Assessment Center (BTAC). Accessed June 27, 2022 at: https://www2.fbi.gov/hq/isd/cirg/ncavc.htm#bau

Hawaii Revised Statutes; *Chapter 323B, Health Care Privacy Harmonization Act*

Hawaii Revised Statutes; *Chapter 487R-2, Destruction of personal information records*

Hawaii Revised Statutes; *Chapter s 846 and 846D, Uniform Employee and Student Online Privacy Protection Act*

McCain Institute. Accessed July 1, 2022 at: https://www.mccaininstitute.org/programs/preventing-targeted-violence/

National Governors Association; State Targeted Violence Prevention: Programming & Key Performance Indicators (April 25, 2022). Accessed August 16, 2022: https://www.nga.org/center/publications/state-targeted-violence-prevention-programming-key-performance-indicators/

National Threat Assessment Center (NTAC). Accessed June 27, 2022 at: http://www.secretservice.gov/ntac

- *Hot Yoga Tallahassee: A Case Study of Misogynistic Extremism* (March 2022).
- *Averting Targeted School Violence: A U.S. Secret Service Analysis of Plots Against Schools* (March 2021).
- *Mass Attacks in Public Spaces – 2019* (August 2020).
- *Protecting America's Schools: A U.S. Secret Service Analysis of Targeted School Violence* (November 2019).
- *Enhancing School Safety Using a Threat Assessment Model: An Operational Guide for Preventing Targeted School Violence* (July 2018).

U.S. Department of Justice's Global Justice Information Sharing Initiative; *Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development Template* (March 2019). Accessed August 25, 2022 at: https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_pcrcl_policy_development_template_v_3.0_march_2019.pdf#page=5&zoom=100,93,316

Appendix B – Definitions

Attack means any attack or series of attacks by anyone causing, or which may cause, damage or injury to persons or property in the United States in any manner by the use of chemical, biological, radiological, nuclear, explosives, firearms, cyber, or other weapons or processes; and any form of hostile action[6].

Bodily injury[7] means physical pain, illness, or any impairment of physical condition.

Disruption to agency operations includes but is not limited to obstructing government operations as defined in HRS § 710-1010, or physical inconvenience, alarm by persons present on agency premises and/or employed by the agency, hazardous or physically offensive conditions, or impeding or obstructing movement on agency premises except in connection with a labor dispute[8].

Domestic Terrorism means activities that involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; Appear to be intended to:

1. to intimidate or coerce a civilian population;
2. to influence the policy of a government by intimidation or coercion; or
3. affect the conduct of a government by mass destruction, assassination, or kidnapping; and occur primarily within the territorial jurisdiction of the United States[9].

Homeland security means a concerted effort to:

- *Prevent terrorist attacks within the United States;*
- *Reduce the State's vulnerability to attacks and terrorist activities; and*
- *Minimize the damage and recover from attacks that occur[10].*

Serious bodily injury[11] means bodily injury which creates a substantial risk of death, or which causes serious, permanent disfigurement, or protracted loss or impairment of the function of any bodily member or organ.

Substantial bodily injury[11] means bodily injury which causes:

1. A major avulsion, laceration, or penetration of the skin;
2. A burn of at least second-degree severity;
3. A bone fracture;
4. A serious concussion; or
5. A tearing, rupture, or corrosive damage to the esophagus, viscera, or other internal organs.

Targeted violence[13] means acts dangerous to human life that are in violation of the criminal laws of the United States or of any State and that: a) involve a degree of planning and b) involve a pre-identified target including: i) individual(s) based on actual or perceived identity traits or group affiliation or ii) property based on actual or perceived identity traits or group affiliation; and 2. appears intended to: a) intimidate, coerce, or otherwise impact a broader population beyond the target(s) of the immediate act; or b) generate publicity for the perpetrator or his or her grievances; and 3. occurs within the territorial jurisdiction of the

United States; and 4. excludes acts of interpersonal violence, street or gang-related crimes, or financially motivated crimes.

Terrorism means an act that is dangerous to human life or potentially destructive of critical infrastructure; and is a violation of the criminal laws of the U.S., or any state or other subdivision of the U.S.; AND appears to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by mass destruction, assassination, or kidnapping[13].

Threat assessment[14] means a product or process of evaluating information based on a set of criteria for entities, actions, or occurrences, whether natural or human-made, that have or indicate the potential to harm life, information, operations and/or property[15].

SOURCES

1. Robert A. Fein and Bryan Vossekuil, *Protective Intelligence & Threat Assessment Investigations: A Guide for State and Local Law Enforcement.* (Washington, DC, United States Department of Justice, Office of Justice Programs, National Institute of Justice, 2000); Randy Borum, Robert Fein, Bryan Vossekuil, and John Berglund, *Threat Assessment: Defining an Approach for Evaluating Risk of Targeted Violence.* Behavioral Sciences & the Law 17, no. 3 (1999): 323-337; Bryan Vossekuil, Robert A. Fein, and John M. Berglund, Threat Assessment: Assessing the Risk of Targeted Violence. Journal of Threat Assessment and Management 2, no. 3-4 (2015): 243-254.
2. Florida Department of Law Enforcement, *Florida's Strategy for Targeted Violence Prevention: Behavioral Threat Assessment and Management; Intervention and Prevention.*
3. National Threat Assessment Center. (2021). *Averting Targeted School Violence: A U.S. Secret Service Analysis of Plots Against Schools.* U.S. Secret Service, Department of Homeland Security.
4. HRS §128A https://www.capitol.hawaii.gov/hrscurrent/Vol03_Ch0121-0200D/HRS0128A/HRS_0128A-.htm
5. HRS §128B https://www.capitol.hawaii.gov/hrscurrent/Vol03_Ch0121-0200D/HRS0128B/
6. Sec. 128A, Hawai'i Revised Statutes.
7. Sec. 707-700, Hawai'i Revised Statutes
8. 2022 legislative session proposal, HB 1415.
9. Antiterrorism Act, 18 U.S.C. § 2331 (1990).
10. Sec. 128A, Hawaii Revised Statutes.
11. Sec. 707-700, Hawaii Revised Statutes.
12. Sec. 707-700, Hawaii Revised Statutes
13. The Department of Homeland Security (DHS), Notice of Funding Opportunity (NOFO) Fiscal Year 2022 Targeted Violence and Terrorism Prevention (TVTP) Grant Program. Accessed August 12, 2022 at: https://www.dhs.gov/sites/default/files/2022-04/FY%202022%20TVTP%20Notice%20of%20Funding%20Opportunity.pdf
14. Homeland Security Act, 6 U.S.C. 101(18) (2002).
15. Based on definition found in The Department of Homeland Security (DHS), DHS Lexicon Terms and Definitions (Instruction Manual 262-12-001-01). Accessed August 12, 2022 at: https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf

CONTACT US

Frank Pace
Administrator
frank.j.pace@hawaii.gov

State of Hawai'i Department of Defense
Office of Homeland Security
3949 Diamond Head Rd.
Honolulu, HI 96816

General Inquiries
dod.ohs@hawaii.gov
808-369-3570

Planning and Operations
808-369-3527

Grants
808-369-3524

Statewide Interoperability Coordinator (SWIC)
808-369-3523

Hawaii State Fusion Center
hawaiifusioncenter.org
info@hawaiifusioncenter.org
808-369-3589

Infrastructure Resilience Planning Framework (IRPF)

NOVEMBER 2022 | VERSION 1.1

Infrastructure Resilience Planning Framework (IRPF)

The **Cybersecurity and Infrastructure Security Agency (CISA)** has developed the **Infrastructure Resilience Planning Framework (IRPF)** to enable the incorporation of security and resilience considerations in critical infrastructure planning and investment decisions.

The IRPF is organized as follows:

0. Overview

This section addresses the following:

0.1 INTRODUCTION

0.2 PLANNING FOR RESILIENT INFRASTRUCTURE

0.3 THE INFRASTRUCTURE RESILIENCE PLANNING FRAMEWORK (IRPF)

0.4 ALIGNMENT TO OTHER PROCESSES

0.5 RESOURCES FOR FUNDING AND TECHNICAL ASSISTANCE

0. Overview

0.1 INTRODUCTION

Infrastructure is the backbone of our communities, providing not only critical services (such as water, transportation, electricity, and communications), but also the means for health, safety, and economic growth. These systems often extend beyond our communities providing service to entire regions and contributing to the delivery of National Critical Functions. Given the vital importance of infrastructure to our social and economic well-being, it is imperative we ensure our networks are strong, secure, and resilient. In order for communities to thrive in the face of uncontrollable circumstances and adapt to changing conditions (e.g., evolving security threats, impacts from extreme weather, technological development, and socio-economic shifts), we must work to make our infrastructure more resilient.

Presidential Policy Directive 21 (PPD-21) – Critical Infrastructure Security and Resilience defines resilience as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Infrastructure resilience depends on both physical attributes of engineered infrastructure systems and on the capabilities of organizations affecting the operation and management of those systems (e.g., infrastructure owners and operators, regulatory authorities, and vendors and contractors). Resilience is also influenced by organizational factors such as the existence of business continuity and emergency response plans, the level of workforce training, and the frequency of exercises to test plans. Developing resilience is essential to managing the wide range of risks that communities face, including those presented by dependencies between and among infrastructure systems.[1]

The Cybersecurity and Infrastructure Security Agency (CISA) developed the Infrastructure Resilience Planning Framework (IRPF) to provide an approach for localities, regions, and the private sector to work together to plan for the security and resilience of critical infrastructure services in the face of multiple threats and changes. The primary audience for the IRPF is state, local, tribal, and territorial governments and associated regional organizations; however, the IRPF can be flexibly used by any organization seeking to enhance their resilience planning. It provides resources for integrating critical infrastructure into planning as well as a framework for working regionally and across systems and jurisdictions.

This framework provides methods and resources to address critical infrastructure security and resilience through planning, by helping communities and regions:

- **Understand and communicate** how infrastructure resilience contributes to community resilience;
- **Identify** how threats and hazards might impact the normal functioning of community infrastructure and delivery of services;
- **Prepare** governments, owners and operators to withstand and adapt to evolving threats and hazards;
- **Integrate** infrastructure security and resilience considerations, including the impacts of dependencies and cascading disruptions, into planning and investment decisions; and
- **Recover** quickly from disruptions to the normal functioning of community and regional infrastructure

For the purpose of this document, “community” should be understood to include not just individual cities or towns, but also multijurisdictional regional authorities conducting planning and stakeholders with common interests or working on a common corridor to enhance the resilience of related infrastructure systems.

0.2 PLANNING FOR RESILIENT INFRASTRUCTURE

The IRPF is not a definitive roadmap, but rather a flexible set of guidance documents and resources to kickstart infrastructure security and resilience planning and incorporate it into existing planning mechanisms.* While the IRPF is structured as a set of sequential steps, the user can choose which steps and sets of resources to more fully

1 Methodology for Assessing Regional Infrastructure Resilience, CISA, 2021, pg. 8-16 https://www.cisa.gov/sites/default/files/publications/DIS_DHS_Methodology_Report_ISD%20EAD%20Signed_with%20alt-text_0.pdf

* Throughout this guide, we provide links to resources developed by partners other than the Federal Government. This information is provided “as is” for informational purposes only. CISA does not provide any warranties of any kind regarding this information. CISA does not endorse any entity, product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA.

consider infrastructure in any existing or on-going planning process. Communities can review the framework to determine where they are in the planning spectrum and choose the guidance and resources that best serve their needs.

Communities with limited time and resources may want to focus on the infrastructure sectors that support critical functions, such as energy, communications, transportation, and water and wastewater systems initially, with the potential to expand later.

Conversely, communities with more time and resources could consider all other critical infrastructure sectors deemed important and/or vital to the continued performance of key social and economic functions integral to the community or regional prosperity.

The IRPF helps users explore dependency relationships between infrastructure systems to better understand infrastructure risk, develop projects and strategies to address it, and identify funding and implementation resources to take action.

Ultimately infrastructure resilience contributes to a more resilient community, and can help develop and maintain a strong, safe, and economically vibrant place to live and work. This can help form a self-reinforcing cycle whereby increased social and economic resilience lead to increased infrastructure resilience and vice versa.

0.3 THE INFRASTRUCTURE RESILIENCE PLANNING FRAMEWORK (IRPF)

The IRPF is designed to be an easy-to-use framework for incorporating critical infrastructure resilience into local, regional, and Tribal plans. It is intended to help communities, regions, and infrastructure owners and operators better understand critical infrastructure risk, identify opportunities to enhance resilience, and inform policy and investment decisions.

Step 1, Lay the Foundation. Communities define and scope the planning effort, form a planning team to execute the effort, and review existing data, plans, studies, maps, and other resources.

Step 2, Critical Infrastructure Identification. Provides guidance to communities on how to identify and prioritize infrastructure and evaluate dependencies among infrastructure systems.

Step 3, Risk Assessment. Walks communities through the process of conducting a risk assessment of critical infrastructure to include evaluating vulnerabilities to threats and hazards, and consequences that may result.

Step 4, Develop Actions. Provides guidance on the development of a strategic action plan for addressing risk and enhancing infrastructure resilience by identifying and prioritizing potential solutions.

Step 5, Implement & Evaluate. Focuses on incorporating infrastructure resilience projects and strategies into community and regional plans and processes for measuring success.

To support these efforts, the IRPF also includes an assortment of resources to assist communities as they move through the various steps of the IRPF.

RESOURCES AVAILABLE!

Throughout this guide, the IRPF provides assistance as indicated by the symbols below. The goal of this is to provide a comprehensive list of resilience planning resources available to all jurisdictions. The IRPF identifies resources by entity (federal, state, non-profit, etc.), eligibility, infrastructure sector, etc.

The IRPF encourages planners to take a functional, system-based approach when considering critical infrastructure. Individual infrastructure assets are only as important as the ultimate function they help provide: it may not matter that a water treatment plant or pumping station is disrupted during an incident, for example, if there are adequate alternatives for providing potable water to the community until that system can be restored. Alternately, infrastructure systems are highly interconnected, and disruption in one may have cascading impacts that affect a range of other infrastructure systems. Because of these two factors, the IRPF encourages planners to consider the critical functions provided by infrastructure systems as well as the dependencies that exist within and between those systems. A strong understanding of these two factors can help planners identify strategies and projects to reduce their risk and make better investments in resilience.

The IRPF can be applied to all 16 sectors of critical infrastructure identified by Presidential Policy Directive 21 (PPD-21) – Critical Infrastructure Security and Resilience, which establishes a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure against physical and cyber threats. PPD-21 identifies 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. These critical infrastructure sectors are listed in Table 1, including a brief description of the typical components that comprise each sector. While PPD-21 takes a national perspective on critical infrastructure systems and assets, these sectors are also relevant at the local, state, and regional level and understanding risk to these systems can improve security, health and safety, and economic growth in your community.

Within every community and region, these sectors provide critical functions through infrastructure systems. These systems are composed of assets that are linked to and reliant on one another, and the continued operation of these systems is dependent not only on their own assets, but also other systems in other sectors. Importantly, nearly all sectors are reliant on energy, water and wastewater, communications, and transportation systems to function. The IRPF helps users examine these infrastructure systems, identify key dependencies within and between them, and incorporate that knowledge into planning.

Table 1. Critical Infrastructure Sectors

CRITICAL INFRASTRUCTURE SECTOR	TYPICAL COMPONENTS
1. Chemical	Facilities that manufacture basic chemicals, specialty chemicals, agricultural chemicals, pharmaceuticals, and consumer products.
2. Commercial Facilities	Publicly- and privately-owned facilities that draw large crowds of people for entertainment and/or media; gaming; lodging; outdoor events; public assembly; real estate; retail; and sports purposes.
3. Communications	Voice and data services and/or terrestrial, satellite, and wireless communication networks.
4. Critical Manufacturing	Facilities supporting the manufacture of primary metals, machinery, electrical equipment, appliances, and components, and transportation equipment.
5. Dams	Assets in the sector include dam projects, hydropower plants, navigation locks, levees, dikes, hurricane barriers, mine tailings, and other industrial waste impoundments. The National Inventory of Dams lists more than 100,000 dams throughout the United States. A large and diverse set of public and private entities own and operate these facilities under highly distributed regulatory oversight from federal, state, and local entities.
6. Defense Industrial Base	Laboratories, special purpose manufacturing facilities, organizations, and supply chains that perform research and development, design, manufacturing, systems integration, maintenance and servicing of military weapon systems, subsystems, components, subcomponents, or parts that support military operations.
7. Emergency Services	Facilities, communications structures, other specialized equipment supporting/housing law enforcement, fire and rescue services, emergency medical services, emergency management, and public works.
8. Energy	Facilities and systems for electricity generation, transmission, and distribution, and for oil and natural gas extraction, refining, and distribution.
9. Financial Services	Depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions.
10. Food and Agriculture	Areas or facilities associated with the production, processing, and delivery of consumable products (e.g., restaurants, food outlets, food facilities, and farms).
11. Government Facilities	Facilities owned or leased by federal, state, local, territorial, and tribal governments, as well as government and private sector-owned education facilities and national monuments and icons.
12. Healthcare & Public Health	Public and private healthcare facilities, research centers, suppliers, manufacturers, and other physical assets.
13. Information Technology	Physical assets and virtual systems and networks involved in creating information technology products and services, such as research and development, manufacturing, distribution, upgrades, and maintenance.
14. Nuclear Reactors, Materials, and Waste	Nuclear power reactors and their facilities, research and test reactors, cooling ponds, and fuel cycle facilities.
15. Transportation Systems	Aviation, terrestrial or maritime transportation systems (e.g., mass transit, ships, railroad, roadways, and pipeline systems).
16. Water/Wastewater Systems	Potable water systems, wells and wastewater treatment systems.

0.4 ALIGNMENT TO PLANNING EFFORTS AND FEDERALLY RECOGNIZED PROCESSES

It is important to note that the IRPF was developed to align with and inform other federal, state, local, tribal, and territorial planning efforts a community may be responsible for executing. Table 2 identifies some of the existing planning efforts which the IRPF can inform.

The steps and the associated resources can be easily integrated into other planning processes, such as comprehensive, hazard mitigation, environmental, capital improvement programming, and regional transportation. In fact, a key benefit of the IRPF is that it can help identify resilience projects that can be incorporated into these plans, allowing a community to build its resilience over the long-term and providing a prioritized list of potential projects that can be implemented with Federal funding following a disaster. Additionally, the IRPF aligns with and supports the Federal Emergency Management Agency (FEMA) National Mitigation Investment Strategy and the U.S. Government Accountability Office (GAO) Disaster Resilience Framework. While FEMA has established a series of "community lifelines" that, at first, may seem to be at odds with CISA's sector-based approach, these two frameworks are in fact complementary. The community lifelines established by FEMA align with CISA's infrastructure sectors and are intended to support response operations, whereas CISA's 16 sectors can support steady-state activities.

Table 2. Planning Efforts the IRPF Can Inform

EXISTING FEDERAL, STATE, LOCAL, TRIBAL & TERRITORIAL PLANS	
Capital Improvement Plans	Land Use Plans
Comprehensive/General Plans	Long-Term Recovery Plans
Economic Development Plans	Pre-Disaster Recovery Plans
Emergency Operations Plans	Specific/Area Development Plans
FEMA Logistics Capability Assistance Tool (LCAT)	Threat and Hazard Identification and Risk Assessment (THIRA)
Growth Management Plans	Transportation Plans
Hazard Mitigation Plans	Watershed Management Plans
Housing Plans	Other local and regional plans

QUICK TIP

The IRPF can support nearly every phase of the hazard mitigation process by providing a deeper dive into critical infrastructure and dependencies, getting infrastructure owners to the table, and analyzing risk from hazards, which can in turn be used by the community to apply for Federal grant funding. For additional resources, please refer to the **Infrastructure Resilience Planning Resources**.

THERE'S A RESOURCE FOR THAT!

Alignment of IRPF to Federal Planning and Risk Management Processes

This matrix illustrates how the IRPF is in alignment with and complimentary to the various other existing federal risk and/or resilience planning processes and guidelines.

View resource in the Infrastructure Resilience Planning Resources.

Methodology for Assessing Regional Infrastructure Resilience

Based on lessons learned from CISA's Regional Resiliency Assessment Program, this assessment methodology provides a common process for assessing and addressing complex infrastructure resilience issues validated through a decade of RRAP project experience.

View resource in the Infrastructure Resilience Planning Resources.

In many ways, the IRPF complements and supplements other resilience guides and methodologies. For example, outputs from the IRPF can inform Step 3, Risk Assessment, and Characterizing the Built Environment of the National Institute of Standards and Technology (NIST) Community Resilience Planning Guide (CRPG). In addition, the infrastructure resilience assessment process documented in CISA's Methodology for Assessing Regional Infrastructure Resilience closely aligns with the planning steps and guidance outlined in the IRPF.

0.5 RESOURCES FOR FUNDING OPPORTUNITIES AND TECHNICAL ASSISTANCE

A key feature of planning is determining resource availability to develop and carry out planning and implementation. The IRPF provides a compendium of these resources in both a document and a user-friendly matrix, outlining funding opportunities and technical assistance that can help communities make planning a reality.

THERE'S A RESOURCE FOR THAT!

Compendium of Programs and Mechanisms for Funding Infrastructure Resilience

The Compendium of Programs and Mechanisms for Funding Infrastructure Resilience provides a list of potential funding and technical assistance sources with links.

View resource in the Infrastructure Resilience Planning Resources.

1. Lay the Foundation

This section addresses the following:

1.1 IDENTIFY A PROJECT CHAMPION

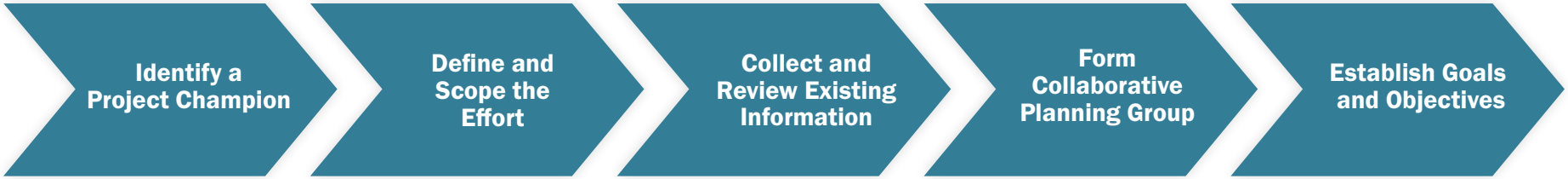
1.2 DEFINE AND SCOPE THE EFFORT

1.3 COLLECT AND REVIEW EXISTING INFORMATION

1.4 FORM COLLABORATIVE PLANNING GROUP

1.5 ESTABLISH GOALS AND OBJECTIVES

1. Lay the Foundation



Step 1 of the IRPF lays the foundation for success by providing guidance on how to develop initial buy-in, form a collaborative planning group, and collect and review existing data, plans, studies, maps, or other technical resources that may be relevant in informing the planning effort. While this section is structured as a sequential process, many of these "steps" occur simultaneously and iteratively. For example, as a champion and planning team are identified, users may wish to revisit their scope and re-evaluate what past assessments and planning activities are relevant to their current effort. Planners should consider how the IRPF can best supplement their current planning process, and which steps will add the most value. Ultimately, the framework is intended to be flexible--users are encouraged to adapt the IRPF process as best meets their needs.

1.1 IDENTIFY A PROJECT CHAMPION

To develop buy-in, it is important that an individual entity who champions the importance of resilience provide support in the form of time and resources to the planning effort. This champion can be a state division, tribal council, local jurisdiction, community planning department, regional planning organization, public/private non-profit, or other organization who is leading the development of a plan. What is important, is that this entity is able to actively support the planning process and implementation efforts.

1.2 DEFINE AND SCOPE THE EFFORT

Prior to integrating the IRPF into a planning process, several questions should be considered to define the effort:

- What is driving the desire or need for resilience planning?
- What are the community's resilience goals and objectives?
- Are there specific shortcomings in infrastructure serving the community that need to be addressed?

There are many types of assessments and analysis that can inform planning, from threat, vulnerability, and criticality analysis, system mapping and diagramming, to modeling and simulation analysis. Defining clear goals, objectives, and scope can help planners determine what forms of analysis will best support their efforts. The Methodology for Assessing Regional Infrastructure Resilience provides additional detail on analytic methods that planners can use to improve their understanding of infrastructure systems in their community, drawn from more than 10 years of experience and more than 120 unique assessments. Once the overall direction of the effort has been determined, a community can more effectively allocate time, funds, and personnel to match the scope of the effort.

PLEASE NOTE

One critical component of success for the IRPF planning process is **process documentation**. At all stages of the IRPF, coordinating leadership and documenting all planning efforts is very important. Take care to ensure proper note-taking, and try to keep regular backups (with redundancies, if possible) of all relevant files.

1.2.1 Time and Resources

It is important to adequately staff and fund planning efforts such that resources are dedicated commensurate with resilience goals and the complexity of the work entailed in meeting them. In recognition of time and resource constraints that may exist, the IRPF is designed to support and complement existing or ongoing local and regional planning activities. Thus, it is anticipated that nominal additional resources and time will be required to incorporate the infrastructure resilience concepts outlined in the IRPF.

QUICK TIP

Communities may be able to save money by incorporating IRPF processes and resources with existing planning practices being funded by grants or technical assistance, such as hazard mitigation, comprehensive, or economic development planning.

1.2.2 Identify a Planning Team Lead

Strong leadership is needed throughout the IRPF integration process, and a planning team lead should serve as a project manager. In most cases, the lead will be an individual from the project champion entity. At a minimum, the lead should report to the project champion, community officials and others as necessary, to provide progress updates and results of the various activities related to the planning process. Table 3 identifies qualifications for a good planning team lead.

Table 3. Planning Team Lead Qualifications

WHAT MAKES A GOOD PLANNING TEAM LEAD?
1. Working knowledge of local and regional infrastructure, such as public works
2. Understanding of threats and hazards, risks, and consequences
3. Ability to engage a broad spectrum of stakeholders to participate in the planning process and provide expertise on critical infrastructure issues
4. Ability to perform administrative, coordination, and event-planning functions and facilitate planning sessions

1.2.3 Conduct Preliminary Activities

Once the planning team lead has been identified, he/she should conduct preliminary activities to lay the foundation for a successful effort. These activities include:

- Defining the purpose of the effort and identifying its relationship to other community planning efforts
- Defining the scope of the effort (including the planning area)
- Articulating goals and objectives and outlining a strategy for the effort
- Developing a preliminary schedule
- Securing a meeting facility
- Identifying a facilitator to facilitate discussions during planning group meetings (if applicable)
- Identifying stakeholders that have an interest or information critical to the effort

PLEASE NOTE

It can be challenging to get all the right stakeholders together and ensure a diverse range of opinions and interests are considered. It can be helpful to hold a stakeholder assessment or analysis with the project champion to determine the multiple organizations that should be included. Repeating this process as stakeholders are added can create a snowball effect of increasing the effectiveness of outreach.

PLEASE NOTE

Collaboration and Safeguarding Information

Planners should be aware of information sharing concerns and consider how sensitive material will safeguarded. Use common cyber security methods like password protected documents in conjunction with Non-Disclosure Agreements. There are existing resources such as the Congressionally mandated Protected Critical Infrastructure Information (PCII) which is designed to protect private sector infrastructure information voluntarily shared without exposing sensitive data, as well as the Transportation Security Administration (TSA) SSI Program which protects and redacts Sensitive Security Information (SSI).

1.3 COLLECT AND REVIEW EXISTING INFORMATION

To establish a solid foundation for participants, it is important to identify previous planning efforts, studies, mapping, and other data that can inform the effort. These data resources can come from state, local, tribal, and territorial (SLTT), regional, or federal sources.

Prior to the first planning meeting, the planning team lead should identify and review data and information pertinent to the community's infrastructure assets, systems, and networks, as well as data and information on threats, hazards, and disaster events in the community.

Other existing community plans should also be reviewed to identify information pertinent to the current planning effort. See Table 2 in Section 0.2 for a list of community plans to review. During the review, the strategies in these existing plans should be compared to identify any inconsistencies or conflicts that might be resolved through the current planning effort.

QUICK TIP

While overall scope and objectives will be driven by the nature of the planning activity being undertaken, it can help to think through the goals and approach for enhanced consideration of critical infrastructure within the planning process. Several steps can assist in this process:

- **Define knowledge gaps:** At the outset, it can be valuable to articulate the infrastructure resilience knowledge gaps you seek to resolve. In many cases, these knowledge gaps will include determining how critical functions or services are supported by infrastructure systems, what dependencies exist between systems, and which systems are vulnerable to disruption. This process does not have to be exhaustive but can help planners and participants think expansively about the infrastructure systems and issues that should be examined during planning.
- **Refine scope:** Once knowledge gaps have been defined, refining scope can help focus the role of considering infrastructure resilience within your planning process. The scope of the effort should be wide enough to inform planning, but narrow enough that it is commensurate with the timeline and resources associated with the larger planning project.
- **Develop data collection strategy:** Based on scope and identified knowledge gaps, a strategy can be developed to define what information needs to be collected, how and when it will be gathered, and what participants and partners should be involved. Ultimately, the goal of the data collection strategy is to spell out what must be gathered to better understand infrastructure systems and their resilience issues.
- **Develop analysis strategy:** An analysis strategy can help consider how information will be used to support planning goals and consider what resources and methods will be incorporated into the planning process.

THERE'S A RESOURCE FOR THAT!

Data Collection – Sample List of Resources

The Sample List of Existing Resources provides a general overview of potential reference resources, sorted by resource owners/creators. Creators include:

- Local/County/Regional Agencies
- Critical Infrastructure Owners/Operators
- State, Tribal, and Territorial Agencies
- Federal Agencies

The goal of this list is to encourage that planners employing the IRPF framework identify all previous relevant efforts.

View resource in the Infrastructure Resilience Planning Resources.

Comparison of Existing Community Plans

The Plan Integration for Resilience Scorecard is a plan evaluation method developed by Department of Homeland Security (DHS) Science and Technology through its Coastal Resilience Center of Excellence partner at Texas A&M University. The scorecard can help communities evaluate and coordinate their various plans (e.g., transportation, economic development, hazard mitigation, emergency management, etc.) so that they present consistent strategies and work together to reduce vulnerabilities to hazards.

View the resource at this link and in the Infrastructure Resilience Planning Resources.

1.4 FORM COLLABORATIVE PLANNING GROUP

1.4.1 Identify Participants

One approach for incorporating critical infrastructure resilience into planning is to establish a group of external partners that can inform the broader planning effort. Inviting participation from representatives of the groups identified in Table 4 can provide vital insights and perspectives that inform planning efforts and improve resilience. Collaboration is key and can yield the benefits identified in Figure 1.

For the purposes of the IRPF, critical infrastructure stakeholders include community and private sector partners responsible for the planning, design, development, investment in, and operations and management of critical infrastructure assets and systems. This includes elected officials, community leaders, planners, engineers, public works staff, emergency management personnel, business owners and infrastructure operators. Partners from key sectors can provide operational information about their infrastructure systems that can lead to the identification of resilience challenges and options for improving resilience strategies.

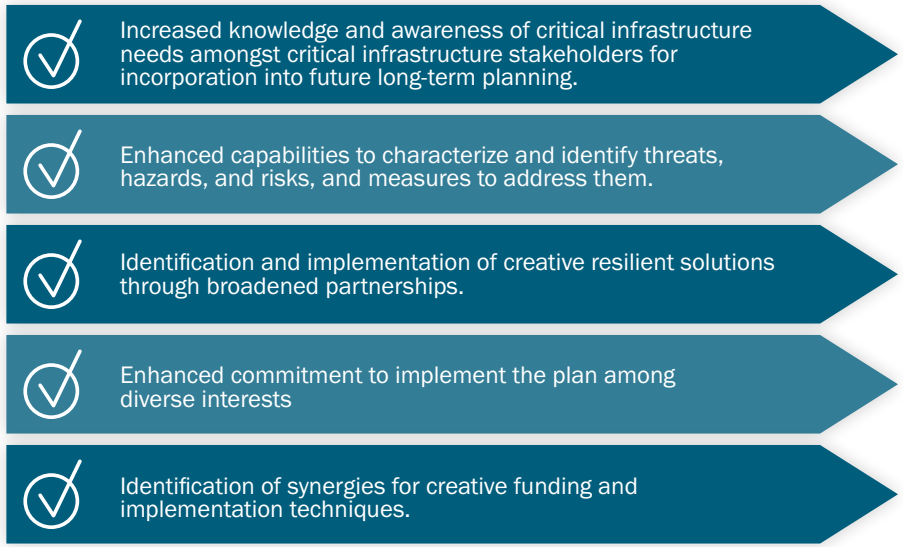


Figure 1. Results of Effective Collaboration

Table 4. Potential Planning Group Participants[2]

POTENTIAL PARTICIPANTS		
KEY SECTORS		
Communications	Information technology/security officers for each communications sector entity IP-based network services Satellite service providers	State and Local Department of Public Safety/Emergency Management Statewide Interoperability Coordinators (SWICs) Telecommunications service providers
Energy	Electric power engineer & cooperatives Energy distribution system provider Energy generation representatives	Information technology/security officers for each energy sector entity Liquid fuel distributor
Transportation	Bridge engineers Information technology/security officers for each transportation sector entity Port/airport authorities Public transit authorities/providers	Railroad representatives Regional Transportation Authorities/Planners State & county Departments of Transportation Traffic engineers
Water and Wastewater	Information technology/security officers for each water/wastewater sector entity Potable water providers Special Utility Districts	Storm water utilities Wastewater treatment plant/systems operators Water Board
GOVERNMENT AND OTHER		
Buildings and Critical Facilities	Building owners Construction firms Critical facility managers	Developers Hospital & healthcare facility representatives Local industry facility managers
City/county Agencies	Building department staff City managers Community planners Economic development agency staff Elected officials	Emergency Management Health department Law enforcement Legal or general council Public works department staff
Region/State Agencies	State/Tribal/Territorial Emergency Management Environmental quality agencies Health departments	Public Utilities Commission Regional/metropolitan planning agency
Federal Agencies	CISA Department of Energy (DOE) Department of Health and Human Services (HHS) Department of Housing and Urban Development (HUD)	Department of Transportation (DOT) Environmental Protection Agency (EPA) FEMA US Army Corps of Engineers

2 Adapted from the NIST Community Resilience Planning Guide

Engagement should include representatives from service providers, including energy, communications, transportation, and water and wastewater, as well as representatives from the wider community who can provide input about critical infrastructure considered essential to the regular functioning of the community.

Federal, state, tribal, and territorial government agency representatives can provide valuable data and information that will be useful in the collection and review of existing data, plans, studies, and mapping resources; the identification of applicable best practices; and the identification of technical assistance and implementation support. Additionally, their participation can provide political support. If these representatives are not able to actively participate, communities can reach out to these representatives as needed and provide periodic updates throughout the planning process.

Cybersecurity should also be considered during the planning process and information technology/security officers or experts that understand the interconnectivity of the cyber infrastructure with the physical infrastructure should be invited to participate. Infrastructure systems and assets increasingly rely on industrial control systems and automated systems that will require cybersecurity expertise to inform planning and investment decisions.

Business risk should be considered in the planning process, so that dependency on critical skills, imports, and other supply chains that are essential to the long-term resilience of the community can be accounted for. This can include discussion with critical infrastructure operators and key businesses. Finding ways to diversify sources proactively will enable the community to be more adaptive as global, national, or local economic conditions change. In November 2020, the Homeland Security Advisory Committee released a report documenting how business risks could impact resilience.

It is important to note that not all participants will be involved in all phases of the planning process. Users should consider when participation will be most valuable to avoid placing undue burden on external partners and ensure efficient collection of relevant information. In addition to active planning team participants, there may be other stakeholders that should be involved in the process. Stakeholders are individuals or groups that are affected by, depend on, and interact with a community's infrastructure. These stakeholders should be engaged to get buy-in and support for the planning process and the final outcomes. However, unlike participants, stakeholders may not be involved in all stages of the planning process, but they provide valuable information on a specific topic or input from different points of view in the community. Stakeholders may include:

- Local businesses and industry representatives
- Critical infrastructure system owners and operators
- Representatives of the community's social institutions (e.g., community organizations, non-governmental organizations, business/industry groups, health, education, environmental, etc.)
- Interested citizens of the community

The planning team lead can develop a mailing/distribution list for these other interested stakeholders to provide them with periodic updates of the progress and outcomes of the planning process and opportunities to provide input/feedback. The planning team lead may also hold interviews with specific stakeholders or groups of stakeholders to garner input during the critical infrastructure identification, risk assessment, and action development steps of the process.

THERE'S A RESOURCE FOR THAT!

Planning Participant Contact Information Sheet

This spreadsheet provides planning officials with a place to keep track of contact information for various stakeholders (including points of contact, phone numbers, email addresses, etc). These stakeholders are sorted by agency/sector type.

View resource in the Infrastructure Resilience Planning Resources.

1.4.2 Invite Participation and Secure Commitments

After identifying prospective participants and gathering relevant contact information, the planning team lead should invite them to participate.

Stakeholders, especially many in private industry may be initially reluctant to participate in planning activities. This can stem from a number of causes, including:

- Concerns about potential regulation
- Business sensitivities and concern about sharing proprietary information
- Competing viewpoints of competitors or other key partners

In communication with private sector partners, it is often valuable to highlight the benefits of improved planning for participants. These include quicker, more effective response and recovery for both their businesses and their customer base, potential insurance savings and reduced costs associated with disaster recovery, improved mitigation activities that can improve the resilience of their upstream and downstream dependencies, and an opportunity to better understand community priorities through planning.

THERE'S A RESOURCE FOR THAT!

Stakeholder Invitation Letter

This sample letter provides the project champion and/or planning team lead with example content for use in inviting and encouraging participation in the planning process. All or portions of the sample content can be used as it best applies to the various types of stakeholders being invited.

View resource in the Infrastructure Resilience Planning Resources.

1.5 ESTABLISH GOALS AND OBJECTIVES

Setting clear goals and objectives is an essential foundation for any successful planning effort as it defines and supports a community's vision of "where it wants to go" or "what it wants to do" with respect to critical infrastructure security and resilience. It is suggested that the planning team lead establish initial goals and objectives based on the high-level goals identified by the project champion and a review of other community plans.

Goals and objectives development should include the full range of planning factors that address critical infrastructure systems as well as other community outcomes, such as livability, sustainability, the economy, the environment, and equity. It is important to consider community goals for economic security and resilience, as well. Sustainable employment and a productive local economy are fundamental resources for supporting the local government and sustaining viable infrastructure resources. The initial goals and objectives can be high level. After performing Step 2 Critical Infrastructure Identification, adjustments can be made to these goals and objectives to make them more specific to the critical infrastructure that the group has identified. Be sure to revalidate these updated goals with the project champion. These goals and objectives can also be further refined at later stages of the IRPF planning process (e.g., alongside the development of an action plan in Step 4).

As the community moves through the iterative planning process, new data, facts, and information may become available, at which time the goals and objectives can be adjusted accordingly. Participants/stakeholders will have an opportunity to validate and refine the goals and objectives based on the findings and determinations from the Critical Infrastructure Identification and Risk Assessment steps of the IRPF.

DEFINITION OF GOALS & OBJECTIVES

Goals are broad statements that describe a desired end state, what the community seeks to achieve through implementing resilience solutions for critical infrastructure.

Objectives are specific, measurable statements that support the achievement of a goal.

THERE'S A RESOURCE FOR THAT!

Sample Goals and Objectives

This list template provides example goals that could guide infrastructure resilience discussions.

View resource in the Infrastructure Resilience Planning Resources.

2. Critical Infrastructure Identification

This section addresses the following:

2.1 IDENTIFY INFRASTRUCTURE

2.2 PRIORITIZE INFRASTRUCTURE

2.3 IDENTIFY DEPENDENCIES

2. Critical Infrastructure Identification

Step 2 includes the identification and prioritization of critical infrastructure in the community and the interdependencies among the infrastructure systems.

2.1 IDENTIFY INFRASTRUCTURE

During planning, it is important to identify infrastructure systems and assets critical to the regular functioning of the community or region. This should include fundamental systems such as energy, water and wastewater, communications, and transportation as well as infrastructure that is critical to the safety, health, and economic vitality of the community. In addition to these sectors, the NIST CRPG also identifies a number of social functions that contribute to a prospering community, including: Community Service, Economy, Education, Family, Government, Health, Media, and Religious & Cultural Beliefs.

Each of these functions comprises its own set of critical infrastructure systems from hospitals and nursing homes to schools and churches, to businesses and community centers. As you work to identify critical infrastructure systems in your community, you should consider what facilities and systems support these societal functions.

ADDITIONAL CONSIDERATIONS FOR IDENTIFYING INFRASTRUCTURE

- Future critical infrastructure systems and assets that are planned or anticipated to support potential future development in the community.
- Infrastructure located across and outside the relevant geographical areas but provide critical services to the community (e.g., transmission lines and pipelines.)
- Critical infrastructure assets, systems, or networks located within the community that may not provide direct services to the community per se, but are critical to the region or Nation at large.

Planning groups should consider creating a database/matrix listing of the community's critical infrastructure to help catalog and analyze infrastructure assets. Beyond serving as an input for establishing dependencies among community infrastructure, the baseline inventory of infrastructure can be used:

- To describe characteristics of existing infrastructure
- To form the basis for a more comprehensive infrastructure identification effort
- To develop mapping products and other visualizations

As you collect information about critical infrastructure systems and assets in your community, it can be entered into local and regional geospatial platforms, enabling visualization and additional analysis.

THERE'S A RESOURCE FOR THAT!

Infrastructure Assets Matrix: Suggested Data Fields Guide

This Guide provides suggested data fields to include in the database/matrix as well as descriptions and key considerations for collecting information about infrastructure assets.

Completing all suggested data fields will help facilitate Federally-supported analyses that the community might wish to undertake in the future. However, the data fields may be modified to best suit the information collection needs of participants/stakeholders and the community.

View resource in the Infrastructure Resilience Planning Resource.

Datasets for Infrastructure Identification

This document provides various datasets to explore sorted by category (Communication, Energy, Transportation, Water, Other, Hazards).

View resource in the Infrastructure Resilience Planning Resource.

2.1.1 Defining Cyber Infrastructure

Communities should understand their reliance on information technology and communications systems required to operate and monitor critical infrastructure and to support key social and economic functions, such as the provision of essential public services and continuity of operations. Cyber infrastructure is essential for the operations and maintenance of critical infrastructure such as power plants, water and wastewater facilities, hospitals, telecommunications systems, oil and gas refineries, and transportation networks. Due to the interconnectedness of physical and cyber infrastructure, community planners and stakeholders who participate in the planning process should have an understanding of the cyber infrastructure assets, systems, and cybersecurity networks that support and ensure the continued operations of infrastructure systems.

Cyber infrastructure includes a wide array of systems that should be considered, such as:

- Computer systems;
- Control systems used to monitor and control a plant or equipment (e.g., Supervisory Control and Data Acquisition (SCADA));
- Networks, such as the Internet;
- Cyber services (e.g., managed security services);
- Data storage and processing systems, including mainframes, cloud providers, server farms, data centers;
- Hardware and software that process, store, and communicate information, or any combination of these elements within electronic information and communications systems; and
- Data and information within electronic information and communications systems.

In considering cyber infrastructure, it is important for planners to consider factors such as the age, origins, upkeep, and locations of remote service providers, so that the full range of challenges to community resilience can be determined.

2.2 PRIORITIZE INFRASTRUCTURE

Having generated a list of critical infrastructure in the community, the planning team lead or a designated facilitator should lead the planning group in prioritizing the identified infrastructure assets. It is suggested that the planning group focus on the impacts each critical infrastructure system/asset has on the community as a means of determining their criticality and priority. Table 5 outlines key impacts to consider. These can be used as criteria with which to prioritize identified critical infrastructure. Communities can decide to use all of the key considerations listed in Table 5 as criteria or simply choose the ones most applicable for their communities. Additionally, communities can modify the key considerations or add their own criteria to best meet their needs.

Table 5. Key Considerations for Prioritizing Infrastructure Systems/Assets

KEY CONSIDERATIONS	DESCRIPTION
Safety Impact	Effect of the system/asset on loss of life, well-being of individuals in the community, the environment, and the physical condition of other infrastructure systems/assets
Context	Value of the system/asset to the identity of the community, region, or Nation; importance of the system/asset as a priority attribute of the community, region, or nation (e.g., primary industry, identifying feature, cultural symbol, etc.)
Operational Impact	Effect of the system/asset on the overall network's ability to operate; the functional impact of the system/asset associated with dependencies that exist within and among systems/assets
Economic Impact	The potential effect on the economic security of the locality, region, or Nation if this infrastructure had a long-term disruption or degradation
Service Impact	Impact of a disruption of the system/asset on the community, region, or a larger critical infrastructure system based on the service it provides to these entities

2.3 IDENTIFY DEPENDENCIES AMONG INFRASTRUCTURE SYSTEMS

The National Infrastructure Protection Plan (NIPP)[3] affirms that "effective risk management requires an understanding of the criticality of assets, systems, and networks, as well as the associated dependencies of critical infrastructure that is essential to enhancing critical infrastructure security and resilience." Dependencies are relationships of reliance within and among infrastructure systems that must be maintained for those systems to function or provide services.[4] Dependencies have a multiplicative effect, as a threat or hazard can result in the loss of services (such as electric outage) which can impact other critical infrastructure using these resources, further impacting other critical infrastructure that depend on them. An impact to a single node or link can result in significant economic and physical damage on a city-wide, regional, and national scale.[5] An improved understanding of dependencies, especially for key infrastructure systems, can inform risk assessment activities and lead to the identification of new priorities for enhancing resilience.

In order to identify dependencies among infrastructure systems, participants should consider:

- **Primary and secondary sources/providers of resources and services required or used by an infrastructure asset to operate.** For example, when considering energy dependency for an infrastructure asset, a community should identify who the electrical power distribution provider is and where the primary and secondary substations for the infrastructure asset are located.
- **Backup sources of resources to sustain operations of the infrastructure asset in the event of a damaging event.** For example, when considering energy and water dependency for an infrastructure asset, a community should identify on-site backup generators and on-site water storage capacity in the event of a significant incident, or change to supply chains.
- **Impacts on downstream infrastructure assets and essential services upon disruption or degradation.** For example, an electric outage could halt operations at a water/wastewater facility as the pumps will not be able to operate and the cyber and information systems will not be able to monitor operations.

3 2013 Plan

4 Adapted from the NIST CRPG. While there are multiple dimensions of dependency—including internal, external, time, space, and source dependencies—the assessment process outlined considers physical and functional relationships between different systems (e.g., drinking water systems require electricity to operate pumps).

5 Argonne National Laboratory, Risk and Infrastructure Science Center, Global Security Sciences Division. "Analysis of Critical Infrastructure Dependencies and Interdependencies, June 2015. ANL/GSS-15/4"

Table 6 provides examples of dependencies that are common among critical infrastructure systems.

Table 6. Examples of Typical Dependencies

DEPENDENCY EXAMPLES
Drinking water systems require electricity to operate pumps
Financial services rely on communications to facilitate transactions and communications systems need power to operate
Crews needed to repair electrical distribution systems need access via roads
Delivery of emergency services depend on communications and roads
Cyber and information technology infrastructure is used to operate and monitor power systems, water/wastewater systems, transportation networks, etc.
Need for a resilient supply of commodities, goods, and services, and manpower to operate businesses and infrastructure

PLEASE NOTE

Some service providers (e.g., energy and communications) may be hesitant to provide system dependency information in a group setting due to information sharing security and liability concerns. Several approaches for identifying lifeline interdependencies are provided in the dependency identification discussion, interview, and worksheet resources to help account for this.

View resources in the Infrastructure Resilience Planning Resources.

THERE'S A RESOURCE FOR THAT!

Infrastructure Dependency Primer

This primer is a web-based, informative resource that provides a foundation for understanding critical infrastructure, identifying dependencies and their impact on communities' risk, and incorporating that knowledge into planning for resilience.

The online primer is publicly accessible at https://www.cisa.gov/idp.

View resource in the Infrastructure Resilience Planning Resources.

Dependency Identification Worksheet

The Dependency Identification Worksheet can assist in documenting the dependencies of the community's infrastructure on other identified critical infrastructure.

The Dependency Identification Worksheet walks communities through a series of questions about an infrastructure asset's dependencies focusing on energy (including electricity and natural gas), communications services, access to key transportation systems, and water and wastewater. Additional questions in the Dependency Identification Worksheet include cyber considerations, such as the data processing systems and services, and consideration of critical products required for functionality/operations, such as chemicals, fuels, raw materials, and removal of byproducts and waste.

View resource in the Infrastructure Resilience Planning Resources.

Community Systems Dependency Discussion Guide

This guide can be used to facilitate a dependency discussion with the planning team, other participants, or stakeholder groups. The guide includes a list of questions to spark conversation and lead to identification of critical community function and/or facility dependencies on infrastructure systems.

View resource in the Infrastructure Resilience Planning Resources.

THERE'S A RESOURCE FOR THAT!

System Owner/Operator Dependency Interview Guide

This guide contains a series of questions that can be used to conduct individual interviews with owners and/or operators of critical infrastructure systems. The questions will help identify and understand the system's dependencies and capabilities to provide service during a disruptive event.

View resource in the Infrastructure Resilience Planning Resources.

Meeting Facilitation Guide

This guide can be used to facilitate a meeting with planning participants to identify community functions, facilities, infrastructure systems, and interdependencies that are most critical to the resilience of the community.

View resource in the Infrastructure Resilience Planning Resources.

3. Risk Assessment

This section addresses the following:

3.1 IDENTIFY THREATS AND HAZARDS

3.2 ASSESS VULNERABILITY

3.3 ASSESS CONSEQUENCES

3.4 INFRASTRUCTURE SYSTEM RISKS

3. Risk Assessment

The Risk Assessment step is a process during which information is collected and values are assigned to risk in order to inform priorities, develop and compare courses of action, and inform decision making. A broad range of risk assessment methodologies are utilized by critical infrastructure stakeholders to understand the most likely and severe incidents that could affect infrastructure assets, systems, and networks. Information resulting from the assessment is utilized to support planning activities and resource allocation.

The Risk Assessment Methodology utilized for the IRPF entails:

1) identifying the threats and hazards to infrastructure,

2) assessing vulnerabilities of prioritized infrastructure,

3) assessing consequences and interactions among infrastructure systems, and

4) prioritizing risk to infrastructure systems.

Once complete, the risk assessment will guide action development and implementation activities.

Critical infrastructure risk assessments often use hypothetical situations or scenarios to divide identified risks into components that can be individually assessed and analyzed. These situations or scenarios consist of an identified threat or hazard, an entity impacted by that threat or hazard, and associated conditions including vulnerabilities and consequences.

UNDERSTANDING RISK*

Risk in the homeland security context is defined as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood (a function of threats and vulnerabilities) and the associated consequences. Resilience is part of the risk equation in that it can influence an entity's vulnerability (or exposure) to different threats and hazards, as well as the consequences that might arise from an event. Ultimately, the process of analyzing risk is important because it shapes decision making on ways to manage risk by accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost. Thus, resilience is fundamentally part of a community's broader risk management strategy.[6]

Threat: Natural, man-made or technological occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Vulnerability: Characteristic of design, location, security posture, operation, or any combination thereof, that renders an entity, asset, system, network, or geographic area susceptible to disruption, destruction, or exploitation.

Consequence (or impact): The effect of an incident, event, or occurrence, whether direct or indirect.

**National Infrastructure Protection Plan*

6 Methodology for Assessing Regional Infrastructure Resilience, CISA, 2021, pg. 15 https://www.cisa.gov/sites/default/files/publications/DIS_DHS_Methodology_Report_ISD%20EAD%20Signed_with%20alt-text_0.pdf

3.1 IDENTIFY THREATS AND HAZARDS TO INFRASTRUCTURE

There are myriad threats and hazards to which infrastructure systems/assets may be exposed. Table 7 identifies potential natural, deliberate, and accidental threats and hazards that should be considered for current and future applicability to priority critical infrastructure.

Table 7. Example Threats & Hazards by Category

NATURAL	ACCIDENTAL	DELIBERATE
Avalanche	Airplane crash	Armed attack
Drought	Cyber incident	Arson/incendiary attack
Earthquake	Dam failure	Biological agent
Extreme cold	HAZMAT release	Chemical agent
Extreme heat	Industrial accident	Civil unrest
Flood	Levee failure	Conventional bomb/improvised explosive device
Hurricane	Mine accident	Cyber incident
Insect infestation	Power failure	Radio spectrum interference
Landslide	Radiological release	Radiological agent
Pandemics	SCADA system failure	Sabotage
Tornado	Train derailment	Theft
Tsunami	Urban conflagration	
Volcanic eruption		
Wildfire		
Winter storm		

**Accidental hazards can be standalone incidents or may be the result of a Deliberate threat or Natural hazard event.*

While all hazards and threats can be considered, communities may want to evaluate the likelihood that each one will occur in order to identify those that should be further assessed for risk. Hazard likelihood can be determined from defined hazard recurrence rates, the frequency of recorded historic events, or good-faith estimations. Sources of information for determining threat/hazard likelihood are identified in Section 3.1.1 and include federal, state, local, tribal, or territorial agencies, as well as colleges and universities. Another valuable source of hazard information is the experience and historical knowledge of planning participants and stakeholders. While it is prudent to prioritize threats/hazards that are most plausible and likely to occur, all hazards can be assessed as time and resources permit.

PLEASE NOTE

It is important to recognize that threat/hazard exposure will change over time, and the type, frequency, or magnitude of impacts may vary from past experience. Factors such as climate, social and economic conditions, the built environment, and technology are dynamic and should be considered when developing threat and hazard context descriptions. Taking future conditions into consideration will yield sound and resilient infrastructure solutions that may change the risk landscape.

3.1.1 Sources of Threat & Hazard Information

Sources of threat and hazard information include:

- Online national weather-related resources, such as the National Climatic Data Center and the Spatial Hazard Events and Losses Database for the United States (SHELDUS)
- Local or regional National Weather Service offices
- Local resources such as the newspaper, chamber of commerce, local historical society, or other resources with records of past occurrences
- Federal and state disaster declaration history
- FEMA Regional Offices

- Emergency management/homeland security agencies
- CISA Regional Protective Security Advisors
- CISA Regional Cybersecurity Advisors
- CISA Interagency Security Committee Regional Advisors
- CISA Chemical Inspectors
- CISA Emergency Communications Coordinators
- United States Computer Emergency Readiness Team (US-CERT)
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- SLTT hazard mitigation offices
- State and major urban area fusion centers
- Tribal governments
- Colleges/universities and other research organizations that have threat and hazard-related programs or extension services

THERE'S A RESOURCE FOR THAT!

Hazard Information and Analysis Resources

Provides external links to hazard information and analysis resources, including single- and multi-hazard data as well as modeling and analytic tools. Includes links from federal programs such as NOAA, USGS, NIFC, and others.

View resource in the Infrastructure Resilience Planning Resources.

Drought and Infrastructure: A Planning Guide

Developed by CISA with the National Drought Resilience Partnership, this guide provides an overview of the drought hazard, examples of direct and indirect impacts it can have on infrastructure systems, and identifies federal resources for assessing and mitigating drought risk.

View resource in the Infrastructure Resilience Planning Resources.

3.1.2 Accounting for Cyber Threats

The cyberspace domain and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. In addition, physical infrastructure systems increasingly include automated control systems, which are at risk to these same cyber threats. Malicious actions seek to exploit vulnerabilities to steal information or money or disrupt, destroy, or threaten the delivery of essential services.

Cyber threat Actors can include:

- Hackers
- Organized Crime
- Terrorist Groups
- State Sponsored / Foreign Intelligence Services

Types of Cyber Attacks can include:

- Web Application Attack
  - SQL Injection
  - Cross-site Scripting
- Phishing
- Spamming
- Application Specific Attacks
- Advanced Persistent Threats
- Malware
  - Adware
  - Bot
  - Ransomware
  - Rootkit
  - Spyware
  - Trojan Horse
  - Virus
  - Worm
- Distributed Denial of Service (DDoS) & Denial of Service (DoS)

3.2 ASSESS VULNERABILITY OF INFRASTRUCTURE

Participants/stakeholders should assess the vulnerability of the prioritized community infrastructure to the identified threats/hazards. A vulnerability assessment involves the evaluation of specific threats and hazards to infrastructure, with the goal of identifying areas of weakness that could result in consequences of concern.

Vulnerability assessments can inform resilience solutions by identifying internal and external factors that may be exploited by adversaries or impacted by hazards and potential points of failure. The identification of problem statements help in the development of actions for enhancing security and resilience. Key elements of vulnerability to consider during the assessment are:

- **Accessibility**: vulnerability of an infrastructure asset based upon its general accessibility to the public.
- **Recognizability**: vulnerability of an infrastructure asset based upon how easily recognizable the asset may be to the public.
- **Recoverability**: ability of an infrastructure asset to easily recover from a disruptive event; a qualitative assessment of the asset's ability to return to normal operations taking into account its dependence on outside services, the capacity at which it is operating, and its own robustness.
- **Susceptibility**: overall vulnerability based on security measures and procedures in place at the infrastructure asset.
- **Proximity**: vulnerability based on an asset's nearness to other susceptible assets.
- **Redundancy**: vulnerability based on whether or not an asset represents a single point of failure within its overall system.

3.3 ASSESS CONSEQUENCES TO INFRASTRUCTURE SYSTEMS

Once the threats and hazards have been identified, participants/stakeholders should consider the likely consequences of those hazards to prioritize critical infrastructure. Consequence is the effect of an event, incident, or occurrence and is commonly measured in four ways:

1. **Human** (injury, illness, or loss of life)
2. **Economic** (costs associated with loss of infrastructure business continuity, and replacement costs)
3. **Mission** (ability of an organization or group to meet a strategic objective or perform a function)
4. **Psychological** (mental or emotional state of individuals or groups resulting in a change in perception and/or behavior)

Consequence factors to consider when assessing risks to the community's infrastructure include security concerns (costs associated with the loss of infrastructure supporting security or defense mission) and additional variables that can cause localized events to turn into broader disruptions (dependencies). Historical events can be used to estimate the resulting disruptions to critical infrastructure.

3.4 INFRASTRUCTURE SYSTEM RISKS

Once the threats have been identified and vulnerabilities and consequences have been assessed, they can be combined to determine the risk to prioritized infrastructure. The planning team should work together to compare each threat/hazard, vulnerability, and consequence scenario in order to prioritize them based on which pose the highest risk.

THERE'S A RESOURCE FOR THAT!

Risk Assessment Methodologies

This resource summarizes various risk analysis methods and provides links to external resources for conducting risk analysis.

View resource in the Infrastructure Resilience Planning Resources.

4. Develop Actions

This section addresses the following:

4.1 REFINE GOALS AND OBJECTIVES

4.2 IDENTIFY RESILIENCE SOLUTIONS

4.3 ASSESS EXISTING RESOURCES AND CAPABILITIES

4.4 SELECT RESILIENCE SOLUTIONS

4.5 DEVELOP IMPLEMENTATION STRATEGIES

4. Develop Actions

This step of the IRPF guides communities through the process of identifying and selecting projects and solutions for enhancing critical infrastructure resilience and developing implementation strategies.

4.1 REFINE GOALS AND OBJECTIVES

Prior to identifying and implementing resilience solutions, communities should revalidate their vision and refine their initial goals and objectives for critical infrastructure resilience in more granularity based on the Critical Infrastructure Identification and Risk Assessment findings.

4.2 IDENTIFY RESILIENCE SOLUTIONS TO MITIGATE RISKS

The core result of the IRPF is risk mitigation solutions for community infrastructure. Resilience solutions can be policies, strategies, plans, codes and ordinances, programs to increase resilience, and/or actual infrastructure projects. The following is a list of resilience-enhancing activities. It is not exhaustive, but rather offers possible points of departure.

- **Utilize Land Use Planning Tools.** Communities can incorporate overlays or new zoning ordinances to restrict infrastructure development/ construction in high hazard areas.
- **Update codes and standards.** Based on the threats, hazards, and vulnerabilities identified through the risk assessment process, communities can update codes and standards to mitigate the greatest risks to community infrastructure. All regulatory updates should include accompanying provisions for enforcement.
- **Invest in robust infrastructure.** Communities can use information generated through the risk assessment process to identify measures that will reduce the vulnerability of key infrastructure to threats and hazards. Potential options include building in spare service capacity, diversifying service networks, diversifying supply chains, designing flexible systems, and reducing service demand through the judicious use of resources.
- **Update infrastructure maintenance and capital improvement programs.** Communities can use the list of prioritized community infrastructure and list of associated dependencies to inform maintenance and renewal priorities for service providers. Existing inspection programs can be augmented to identify infrastructure systems that need improvements that can be prioritized for maintenance.
- **Develop continuity and contingency plans.** Critical infrastructure owners and operators can use information about dependencies to create resourceful, reflective, and flexible continuity plans that help maintain utility services to critical infrastructure during emergency situations. Communities can also use this information to develop effective contingency plans.
- **Incorporate Green Infrastructure.** Consideration of green infrastructure can address climate risk, improve energy efficiency, and reduce resource requirements resulting in not only environmental benefits but also social and economic benefits.

- **Develop an Infrastructure Council.** Consisting of both local government agencies and public and private infrastructure owners and operators, an Infrastructure Council provides a forum for key stakeholders to meet and discuss current activities and issues, dependencies, future development, and opportunities for partnerships and creative funding.

THERE'S A RESOURCE FOR THAT!

Sources for Resilient Solutions

A list of sources for resilient solution ideas is provided in **Infrastructure Resilience Planning Resources**.

FEMA MITIGATION ACTION RESOURCES

Potential mitigation activities are highlighted in the following FEMA resources (located under Resources for Mitigation Activities).

- **Mitigation Ideas: A Resource for Reducing Risk to Natural Hazards** provides examples of mitigation actions that would enhance the resilience of the community's infrastructure to various and specific natural hazards.
- **Mitigation Best Practices Portfolio** provides best practice stories and case studies which offer insight into how other communities have taken action to mitigate against disasters.
- **Hazard Mitigation Planning: Practices for Land Use Planning and Development near Pipelines** provides an overview of risks associated with transmission and distribution pipeline systems and mitigation strategies that can be implemented to reduce these risks.
- **Building Science Branch publications** provide multi-hazard mitigation implementation guidance and ideas for mitigation activities.
- Another resource is **FEMA's Mitigation Action Portfolio** available for download from the Building Resilient Infrastructure and Communities (BRIC) website.

4.2.1 Considering Cybersecurity in Resilience Solutions Identification

Because so much of a community's physical infrastructure is now controlled, in whole or in part, by computers and connected through the internet, planning should consider sound policies and procedures for incorporating cybersecurity improvements into the infrastructure development lifecycle. The following provides some resources to help communities consider cyber threats and take appropriate actions to protect their critical infrastructure.

CYBERSECURITY RESOURCES

- **CISA** is responsible for enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure. Information about CISA's cybersecurity training and education, publications and guidance, alerts and newsletters, technical assistance, and programs and services is included at this link.
- **CISA's cybersecurity assessments** provide a range of products and technical services. Free, voluntary assessments can be requested by partners and range from self-administered surveys to on-site visits.
- **CISA develops and provides a range of information sharing and awareness products**, ranging from threat indicator information to bulletins and advisories. CISA also sponsors sector-based Information Sharing and Analysis Centers as well as Information Sharing and Analysis Organizations to promote the sharing of cyber information and best practices. Additional information can be found at this link.
- **The NIST Cybersecurity Framework** provides voluntary guidance, based on existing standards, guidelines, and practices, for organizations to better manage cybersecurity issues, reduce cybersecurity risk, and mitigate vulnerabilities.
- **The CISA Critical Infrastructure Cyber Community Voluntary Program** helps critical infrastructure owners and operators align with existing resources to assist them in using the Cybersecurity Framework and managing their cyber risks and provides sector-specific guidance and practices.

4.3 IDENTIFY EXISTING RESOURCES AND CAPABILITIES

The action plan can include asking other public and private entities to support implementation to address mutual benefits of resilient infrastructure systems. Identifying and assessing the resources and capabilities of both the community and critical infrastructure owners and operators will help the community prioritize the list of resilience solutions for implementation.

Figure 2 illustrates some of the most common types of existing resources and capabilities that should be considered when prioritizing identification solutions.

Planning & Regulatory authorities	A community is often legally required to abide by or enforce these to ensure public safety, environmental standards, etc. E.g., ordinances, codes, etc.
Existing Plans, Policies & Programs	Can be used as vehicles to incorporate new resilience solutions and expedite implementation as long as there is consistency and alignment with the goals and objectives or the plans, policies, and programs. E.g., comprehensive plans, capital improvement plans
Administrative & Technical Skills within the Community	Knowing existing capabilities within the community helps to identify if and what additional skills or expertise is required for the implementation or resilience solutions.
Financial Resources	Knowing the available financial capabilities and resources that exist to steer and prioritize planning efforts to identify what potential external funding will be required for implementation of resilience solutions. E.g., grants, impact fees, etc.

Figure 2. Common Types of Community Capabilities

THERE'S A RESOURCE FOR THAT!

Sample Capability Assessment Worksheet

A sample capabilities worksheet is provided to assist the community in assessing its existing resources and capabilities. The sample capabilities worksheet can be revised as the community sees fit to suit its needs.

This worksheet asks the planning group to identify all relevant programs and policies in place to assist in the process of resilience oversight. These capabilities are sorted into the following categories: Regulatory, Administrative/Technical, Fiscal, and Utilities. The final pages of the worksheet ask planning group participants to self-assess their degree of capability based on the previous worksheets, and poses a series of additional questions to assist with the self-assessment process.

View resource in the Infrastructure Resilience Planning Resources.

4.4 SELECT RESILIENCE SOLUTIONS FOR IMPLEMENTATION

After producing a list of resilience solutions and identifying capacity, a community should focus their efforts on identifying which public and private entities will need to take action for the goals to be achieved.

An evaluation and prioritization process can help weigh the pros and cons of the different identified resilience solutions. The first step is to develop evaluation criteria for assessing the list of resilience solutions. Criteria consideration should include infrastructure criticality, vulnerabilities, and threat/hazard likelihood, in addition the ability to meet the community goals, objectives, and performance measures.

Additional considerations in evaluating resilience solutions may include:

- Planning and operational requirements of the community and the critical infrastructure owners and operators (e.g., comprehensive/ general plans, emergency operations plans, continuity of operations plans, inspection and maintenance plans, etc.)
- Funding limitations, including operations and maintenance
- Partnership opportunities
- Relevant political priorities
- Community concerns
- Economic impacts

Other evaluation criteria is described in FEMA's Local Hazard Mitigation Planning Handbook. Whatever evaluation criteria are used, they should be agreed upon by planning participants/stakeholders.

THERE'S A RESOURCE FOR THAT!

Mitigation Alternatives Evaluation Questions

This set of questions can be used to support facilitated discussions and qualitatively analyze alternatives for enhancing resilience.

View resource in Infrastructure Resilience Planning Resources.

Economic Evaluation of Solutions

NIST has developed the Economic Decision Guide Software (EDGe$) to help communities evaluate the economic impact (costs and benefits) of resilience investments.

View resource in the Infrastructure Resilience Planning Resources.

Benefit-Cost Analysis (BCA) Toolkit

FEMA has a Benefit-Cost Analysis (BCA) Toolkit that can be used to determine the cost-effectiveness of a mitigation project by weighing the risk reduction benefits of the project against the overall project cost.

The toolkit is available for download at:
fema.gov/grants/guidance-tools/benefit-cost-analysis

CRITERIA FOR EVALUATING SOLUTIONS

FEMA's Local Hazard Mitigation Planning Handbook, March 2013 suggests the following evaluation criteria when analyzing potential solutions:

- **Benefit-Cost:** Are the estimated costs reasonable compared to the probable benefits?
- **Social:** Will the proposed action adversely affect one segment of the population? Will the action disrupt established neighborhoods, break up voting districts, or cause the relocation of lower income people?
- **Life safety:** How effectively will the action protect lives and prevent injuries?
- **Property protection:** How significant will the action be at eliminating or reducing damage to structures and infrastructure?
- **Technical:** Is the resilience solution technically feasible? Is it a long-term solution?
- **Administrative:** Does the community have the personnel and administrative capabilities to implement the resilience solution and maintain it, or will outside assistance be necessary?
- **Political:** Does the public support the resilience solution? Is there political will to support it?
- **Legal:** Does the community have the authority to implement the resilience solution?
- **Environmental:** What are the potential environmental impacts of the resilience solution? Will it comply with environmental regulations?
- **Local champion:** Is there a strong advocate for the action or project among local departments and agencies who will support the action's implementation?
- **Other community objectives:** Does the action advance other community objectives, such as capital improvements, economic development, environmental quality, or open space preservation? Does it support the policies of the comprehensive plan?

4.5 DEVELOP IMPLEMENTATION STRATEGIES

After the resilience solutions are evaluated and prioritized, the community can begin to develop implementation strategies. The implementation strategies describe how each prioritized resilience solution will be implemented and administered by the community. Elements that should be included in the implementation plan are briefly described below:

- **Responsible Party:** A specific agency, department, or position/person should be assigned to carry out the resilience solution.
- **Collaborators/partner agencies/private sector partners:** Other partner agencies or collaborators to assist in the implementation of the resilience solution.
- **Preliminary implementation steps:** Description of the preliminary steps for the implementation of the resilience solution. The responsible person/agency/department and any collaborators/partner agencies can provide input on the preliminary steps for implementation. These steps can be revised over time, as necessary, based on changing conditions, situations, resources, etc.
- **Estimated timeline:** Timeframe for implementation of the resilience solution. The timeframe can detail when the resilience solution will be started and when it should be fully implemented.
- **Resources required for implementation:** Resources include funding, technical assistance, personnel, and materials.
- **Potential barriers to implementation and potential solutions:** Description of potential barriers to implementation and potential solutions to overcome those barriers.

THERE'S A RESOURCE FOR THAT!

Resilient Solution Strategy Worksheet

The Resilience Solution Strategy Worksheet is a sample worksheet that communities can use to fill out implementation strategy elements for each resilience solution.

View resource in the Infrastructure Resilience Planning Resources.

5. Implement & Evaluate

This section addresses the following:

5.1 IMPLEMENT THROUGH EXISTING PLANNING MECHANISMS

5.2 MONITOR AND EVALUATE EFFECTIVENESS

5.3 UPDATE PLANS

5. Implement & Evaluate

This section provides information on how communities can implement the prioritized resilience solutions through existing community planning mechanisms, and potential funding and technical assistance sources.

THERE'S A RESOURCE FOR THAT!

IRPF Plan Integration

This document provides an overview of possible integrations with other community planning efforts/processes.

View resource in the Infrastructure Resilience Planning Resources.

5.1 IMPLEMENT THROUGH EXISTING PLANNING MECHANISMS

One of the best ways for communities to succeed in reducing risks from threats and hazards in the long term is to integrate the prioritized resilience solutions in existing community plans, policies, and programs. Planning participants and other community stakeholders should review the community's operations, priorities, and existing planning mechanisms to see how and where resilience projects and strategies can be integrated. Some examples of existing plans and programs in which resilience solutions can be integrated include:

- Capital Improvement Plans
- Comprehensive/General Plans
- Economic Development Plans
- Emergency Communications Plans
- Emergency Operations Plans
- FEMA Hazard Mitigation Plans
- FEMA Threat and Hazard Identification and Risk Assessment (THIRA)
- Growth Management Plans
- Housing Plans
- Land Use Plans
- Long-Term Recovery Plans
- Other community-specific plans
- Pre-Disaster Recovery Plans
- Specific/Area Development Plans
- Transportation Plans
- Watershed Management Plans

5.1.1 Potential Funding and Technical Assistance Sources for Implementation

There are several ways a community can fund the implementation of its identified resilient solutions. Sources can include traditional infrastructure mechanisms such as taxes, fees, and bonds, as well as grants from federal and state government agencies and philanthropic organizations.

In a time of limited resources at all levels of government, communities should also consider public-private partnerships to develop innovative financing mechanisms. These mechanisms bring additional resources to bear for infrastructure development and can create efficiencies by distributing risks across many parties.

Various departments and agencies at the Federal and SLTT level, as well as non-profit and professional organizations may also provide technical assistance. Technical assistance is the provision of technical expertise to assist a community in the design and development of community infrastructure projects incorporating best practices with respect to resilience enhancements.

5.2 MONITOR, EVALUATE, AND ASSESS EFFECTIVENESS

All plans should have maintenance procedures developed by the community to monitor, evaluate, and assess the effectiveness of the resilience solutions in meeting the community goals and objectives. Measuring performance provides a foundation for subsequent solution and plan modification in the future.

Exercises may be one way to evaluate the effectiveness of operational plans and resilience solutions. The CISA Tabletop Exercise Package (CTEP) is a resource that can be used by communities and critical infrastructure stakeholders to develop and conduct exercises of plans and procedures.

THERE'S A RESOURCE FOR THAT!

Compendium of Programs and Mechanisms for Funding Infrastructure Resilience

The Compendium of Programs and Mechanisms for Funding Infrastructure Resilience provides a list of potential funding and technical assistance sources with links.

View resource in the Infrastructure Resilience Planning Resources.

In addition to this compendium, the FEMA Hazard Mitigation Assistance Grants page provides additional detail and information about FEMA grants.

KEY CONSIDERATIONS FOR EVALUATING PLANS

- Have the nature or magnitude of the threats or hazards changed?
- Are there new threats or hazards affecting the community?
- Do the identified goals, objectives, and solutions address current and expected risk conditions?
- Have the resilience solutions been implemented and completed?
- Has the implementation of solutions resulted in expected outcomes?
- Are current resources adequate to implement solutions?
- What other resources are needed to implement the solutions?
- What factors have resulted in successful implementation of solutions?
- What obstacles to implementation have you encountered? What can be done to overcome these obstacles?

5.2.1 Develop Framework to Monitor, Evaluate, and Assess Effectiveness of Resilience Solutions

Communities should develop a framework for monitoring, evaluation, and assessment of the effectiveness of planning efforts. At a minimum, planners should identify:

- **Responsible party:** Who or what agency will be responsible for monitoring implementation? Who or what agency will coordinate the monitoring and evaluation process?
- **Schedule:** When will resilience planning and implementation efforts be evaluated?
- **Process:** What is the process or method in which plans will be monitored and evaluated? What criteria will be used to evaluate the effectiveness of resilience solutions?

5.3 UPDATE PLANS

Communities should include a process for updating their plans. As a community monitors, evaluates, and assesses the effectiveness of its planning activities, there will be feedback based on successes, obstacles encountered, and lessons learned that can be incorporated into future efforts. The community should consider who or what agency will lead and coordinate a plan update, as well as how and when an update process should be initiated.

The update schedule may be accelerated following a disaster event or concurrent with the development of a recovery or post-disaster redevelopment plan. This allows the community to address subsequent changes in vulnerabilities and priorities, goals, and objectives following a disaster event. Additional funding sources will be available after a disaster event that communities will be able to leverage for implementation of resilience solutions. Communities should also leverage the greater public awareness and interest in resilience after a disaster event and incorporate infrastructure resilience into additional community planning efforts and strategies.

KEY REASONS FOR UPDATING PLANS

- Changes in community development, such as new, recent or potential development or demographic changes that would impact infrastructure requirements.
- The occurrence of a major incident/disaster.
- Changes in operational resources (policy, personnel, facilities, equipment, or organizational structure) that would impact development or maintenance/operations of infrastructure systems.
- Changes in guidance or standards for the development or maintenance and operations of infrastructure systems.
- Changes in political priorities that would impact buy-in or support for the implementation of resilient solutions to enhance the community's infrastructure systems.
- Changes in the acceptability of various risks and major disruptions to infrastructure systems.

All Resources

This section includes resources for:

OVERVIEW

STEP 1: LAY THE FOUNDATION

STEP 2: CRITICAL INFRASTRUCTURE IDENTIFICATION

STEP 3: RISK ASSESSMENT

STEP 4: DEVELOP ACTIONS

STEP 5: IMPLEMENT & EVALUATE

Overview

ALIGNMENT OF IRPF TO FEDERAL PLANNING AND RISK MANAGEMENT PROCESSES

Format: Matrix

Type: PDF

Pages: 2

Summary: This matrix illustrates how the Infrastructure Resilience Planning Framework is in alignment with and complimentary to the various other existing federal risk and/or resilience planning processes and guidelines.

[VIEW PDF]

METHODOLOGY FOR ASSESSING REGIONAL INFRASTRUCTURE RESILIENCE

Format: Document

Type: PDF

Pages: 118

Summary: Based on lessons learned from CISA's Regional Resiliency Assessment Program, this assessment methodology provides a common process for assessing and addressing complex infrastructure resilience issues validated through a decade of RRAP project experience.

[VIEW PDF]

Step 1. Lay the Foundation

DATA COLLECTION SAMPLE LIST OF RESOURCES

Format: Table

Type: PDF document with embedded tables

Pages: 2

Summary: Provides general overview of potential reference resources, sorted by resource owners/creators. Creators include: Local/County/Regional Agencies, Critical Infrastructure Owner/Operator, State Agencies, Federal Agencies. List assists planners in the process of employing the IRPF to identify all previous relevant efforts.

[VIEW PDF]

COMPARISON OF EXISTING COMMUNITY PLANS

Format: Guidebook

Type: Online PDF

Pages: 142

Summary: The Plan Integration for Resilience Scorecard is a plan evaluation method developed by DHS Science and Technology through its Coastal Resilience Center of Excellence partner at Texas A&M University. The scorecard can help communities evaluate and coordinate their various plans (e.g., transportation, economic development, hazard mitigation, emergency management, etc.) so that they present consistent strategies and work together to reduce vulnerabilities to hazards.

[RESOURCE LINK]

PLANNING PARTICIPANT CONTACT INFORMATION SHEET

Format: Template (data sheet)

Type: PDF document

Pages: 2

Summary: This spreadsheet provides planning officials with a place to keep track of contact information for various planning group participants (including points of contact, phone numbers, email addresses, etc). These stakeholders are sorted by agency/sector type.

[VIEW PDF]

STAKEHOLDER INVITATION LETTER

Format: Template (letter)

Type: PDF document

Pages: 1

Summary: This sample letter provides the project champion and/or planning team lead with example content for use in inviting and encouraging participation in the planning process. All or portions of the sample content can be used as it best applies to the various types of stakeholders being invited.

[VIEW PDF]

SAMPLE GOALS AND OBJECTIVES

Format: Template (list)

Type: PDF document

Pages: 2

Summary: This template lists more goals that could guide infrastructure resilience discussions.

[VIEW PDF]

Step 2. Critical Infrastructure Identification

INFRASTRUCTURE ASSETS MATRIX: SUGGESTED DATA FIELDS

Format: Table

Type: PDF document with embedded table

Pages: 3

Summary: This table identifies key data collection suggestions for critical infrastructure asset assessment. Data fields include relevant contact information, owner names, latitude/longitude, type, status, and more.

[VIEW PDF]

INFRASTRUCTURE DEPENDENCY PRIMER

Format: Website

Type: Online Website

Pages: -

Summary: The Infrastructure Dependency Primer is an online, educational supplement to the IRPF and aims to answer fundamental questions planners and decision-makers may have, including:

- *What are infrastructure dependencies and why should I care?*
- *What is resilience, how does it relate to dependencies, and how do I plan for it?*
- *What resources are there to help me reduce dependency risks and enhance the resilience of my community?*

This web-based resource is publicly accessible to be independently explored by users based on their interests and needs. No prerequisite training or knowledge is needed to benefit from content.

[RESOURCE LINK]

DATASETS FOR INFRASTRUCTURE IDENTIFICATION

Format: Document

Type: PDF document

Pages: 7

Summary: This resource is centered around the Homeland Infrastructure Foundation Level Data (HIFLD). The document provides various datasets to explore sorted by category (Communication, Energy, Transportation, Water, Other, Hazards).

[VIEW PDF]

DEPENDENCY IDENTIFICATION WORKSHEET

Format: Worksheet

Type: Fillable PDF form

Pages: 7

Summary: This worksheet asks planning participants to identify the following potential dependencies for each infrastructure asset: energy, natural gas, communications, transportation, water, wastewater, cyber, and critical products.

[VIEW PDF]

COMMUNITY SYSTEMS DEPENDENCY DISCUSSION GUIDE

Format: Guide

Type: PDF document

Pages: 2

Summary: This guide can be used to facilitate a dependency discussion with the planning team, other participants, or stakeholder groups. The guide includes a list of questions to spark conversation and lead to identification of critical community function and/or facility dependencies on infrastructure systems.

[VIEW PDF]

SYSTEM OWNER/ OPERATOR DEPENDENCY INTERVIEW GUIDE

Format: Guide

Type: PDF document

Pages: 1

Summary: This guide contains a series of questions that can be used to conduct individual interviews with owners and/or operators of critical infrastructure systems. The questions will help identify and understand the system's dependencies and capabilities to provide service during a disruptive event.

[VIEW PDF]

MEETING FACILITATION GUIDE

Format: Guide

Type: PDF document

Pages: 2

Summary: This guide can be used to facilitate a meeting with planning participants to identify community functions, facilities, infrastructure systems, and interdependencies that are most critical to the resilience of the community.

[VIEW PDF]

Step 3. Risk Assessment

HAZARD INFORMATION AND ANALYSIS RESOURCES

Format: Table with external links

Type: PDF document with embedded table

Pages: 4

Summary: Provides external links to hazard information and analysis resources, including single- and multi-hazard data as well as modeling and analytic tools. Includes links from federal programs such as NOAA, USGS, NIFC, and others.

[VIEW PDF]

DROUGHT AND INFRASTRUCTURE: A PLANNING GUIDE

Format: Guide

Type: PDF document

Pages: 10

Summary: Developed by CISA with the National Drought Resilience Partnership, this guide provides an overview of the drought hazard, examples of direct and indirect impacts it can have on infrastructure systems, and identifies federal resources for assessing and mitigating drought risk.

[VIEW PDF]

RISK ASSESSMENT METHODOLOGIES

Format: Guide

Type: PDF document with images and external links

Pages: 6

Summary: Summarizes the NIST CRPG risk analysis process. Provides links to external resources for conducting risk analysis, including:

- Seismic Hazards
- Sea Level Rise and Coastal Flooding
- Floods
- Landslides
- What-If Hazard Analysis
- Sector-Specific Plans (SSPs) Analysis
- Infrastructure Survey Tool (IST)
- Integrated Rapid Visual Screening (IRVS)
- FEMA's HAZUS-MH
- Methodology for Assessing Regional Infrastructure Resilience

[VIEW PDF]

Step 4. Develop Actions

SOURCES FOR RESILIENT SOLUTIONS

Format: Table with external links

Type: PDF document with embedded table

Pages: 9

Summary: Provides a list of sources with external links for resilience solution ideas sorted by disaster type. Provides short description for each link.

[VIEW PDF]

SAMPLE CAPABILITY ASSESSMENT WORKSHEET

Format: Worksheet

Type: Fillable PDF form

Pages: 6

Summary: This worksheet asks planning participants to identify all relevant programs and policies in place to assist in the process of resilience oversight. These capabilities are sorted into the following categories: Regulatory, Administrative/ Technical, Fiscal, and Utilities. The final pages of the worksheet ask planning participants to self-assess their degree of capability based on the previous worksheets, and poses a series of additional questions to assist with the self-assessment process.

[VIEW PDF]

MITIGATION ALTERNATIVES EVALUATION GUIDE

Format: Guide

Type: PDF document

Pages: 1

Summary: Questions that can be used to support facilitated discussions and qualitatively analyze alternatives for enhancing resilience.

[VIEW PDF]

NIST ECONOMIC DECISION GUIDE SOFTWARE (EDGE$)

Format: Software

Type: Online software

Pages: -

Summary: NIST has created the Economic Decision Guide Software (EDGe$) to help evaluate the economic impact of investments. The resource helps to identify and compare the relevant present and future resilience costs and benefits associated with new capital investment. EDGe$ can be found at **edges.nist.gov**

[RESOURCE LINK]

RESILIENT SOLUTION STRATEGY WORKSHEET

Format: Worksheet

Type: Fillable PDF form

Pages: 3

Summary: This sample worksheet can be used by communities to fill out implementation strategy elements for each identified resilience solution.

[VIEW PDF]

Step 5. Implement & Evaluate

PLAN INTEGRATION

Format: Table

Type: PDF document with embedded table

Pages: 3

Summary: Provides an overview of possible integrations with other community planning efforts/processes. General suggestions.

[VIEW PDF]

COMPENDIUM OF PROGRAMS AND MECHANISMS FOR FUNDING INFRASTRUCTURE RESILIENCE

Format: Guide

Type: PDF document

Pages: 40

Summary: The IRPF provides a compendium of available funding and resources on a document outlining funding opportunities and technical assistance that can help communities make planning a reality.

[VIEW PDF]

Glossary

This section includes the following:

KEY TERMS

ABBREVIATIONS & ACRONYMS

CRITICAL INFRASTRUCTURE SECTORS

Key Terms

TERM	DEFINITION
Community	One or more local jurisdictions or special districts representing a region or shared infrastructure corridor.
Consequence	The effect of an event, incident, or occurrence and is commonly measured in four ways: Human, Economic, Mission, and Psychological.
Critical Infrastructure	Assets, systems, and networks, both physical and virtual, so regionally or nationally vital that their incapacitation or destruction would have a debilitating effect on security, the economy, public health or safety, or any combination thereof.
Criticality	A measure of the importance associated with the loss or degradation of infrastructure.
Cyber Infrastructure	Electronic information and communications systems and services.
Dependency	Relationship of reliance within and among infrastructure systems that must be maintained for those systems to function or provide services. Dependencies can be bi-directional in nature.
Evaluation	Assessing the effectiveness of planning at achieving its stated goals, objectives, and performance measures.
Facilitator	Individual or entity responsible for convening stakeholders and managing dialogue to result in plans and commitments to action. May also serve as the planning team lead.
Goal	Broad statement that describes a desired end state, what the community seeks to achieve through implementing resilience solutions for critical infrastructure.
Man-made Hazard	Criminal or terrorist attack such as an explosive, biological, cyber, or chemical agent that have the potential to disrupt or exploit the community's infrastructure.
Mitigation	The capabilities necessary to reduce loss of life and property by lessening the impact of disasters.
Monitoring	Tracking the implementation of the prioritized resilient solutions.
Natural Hazard	Weather and geological events, such as flood, hurricane, tornado, or earthquake that have the potential to disrupt or incapacitate the community's infrastructure.

TERM	DEFINITION
Objective	Specific, measurable statement that supports the achievement of a goal.
Physical Infrastructure	Tangible structures or facilities and components that provide infrastructure sector services to communities or regions providing services.
Planning Framework	Steps communities can follow to develop a strategy or list of prioritized actions that enhance the security and resilience of critical infrastructure.
Planning group	Group of individuals within the community from various sectors, agencies, and organizations who add value to the resilience planning process and remain committed throughout the effort.
Planning Team Lead	The key personnel that is involved in and drives the infrastructure resilience planning process throughout and has a working knowledge and understanding of local threats, hazards, and infrastructure. May be dual-hatted as the "facilitator".
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.
Risk	The potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence, often measured and used to compare different future situations.
Risk Assessment	An evaluation that considers the types of threats and hazards that threaten community infrastructure systems and weighs vulnerable community infrastructure.
Stakeholder	A stakeholder is a party or entity that delivers, depends on, or is affected by infrastructure service or facility operations, plans or decisions under consideration.
Technological Hazard	Accidental human activities, such as dam and levee construction or the manufacture, transportation, storage, and use of hazardous materials that have the potential to disrupt or incapacitate the community's infrastructure.
Threat	Any entity, action, or occurrence, whether natural or man-made, that has or indicates the potential to pose danger to life, information, operations, and/or property.
Vulnerability	Characteristic of design, location, security posture, operation, or any combination thereof, that renders an entity, asset, system, network, or geographic area susceptible to disruption, destruction, or exploitation.

Abbreviations & Acronyms

ACRONYM	DEFINITION
ASCE	American Society of Civil Engineers
CIP	Capital Improvement Plan
CISA	Cybersecurity and Infrastructure Security Agency
CRPG	Community Resilience Planning Guide
CTEP	CISA Tabletop Exercise Package
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DOE	Department of Energy
DOT	Department of Transportation
DoS	Denial of Service
EDGe$	Economic Decision Guide Software
EPA	Environmental Protection Agency
FEMA	Federal Emergency Management Agency
FIRM	Flood Insurance Rate Map
HUD	Housing and Urban Development
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDR	Infrastructure Development and Recovery
IRPF	Infrastructure Resilience Planning Framework

ACRONYM	DEFINITION
IRVS	Integrated Rapid Visual Screening
IST	Infrastructure Survey Tool
LCAT	Logistics Capability Assessment Tool
NIFC	National Interagency Fire Center
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
PPD	Presidential Policy Directive
PSA	Protective Security Advisor
SCADA	Supervisory Control and Date Acquisition
SHELDUS	Spatial Hazard Events and Losses Database
SLTT	State, Local, Tribal, and Territorial
SME	Subject Matter Expert
SRMA	Sector Risk Management Agency
SSP	Sector Specific Plan
THIRA	Threat and Hazard Identification Risk Assessment
US-CERT	United States Computer Emergency Readiness Team
USGS	United States Geological Survey

Critical Infrastructure Sectors

SECTOR	SECTOR RISK MANAGEMENT AGENCY (SRMA)
Chemical	Cybersecurity and Infrastructure Security Agency
Commercial Facilities	Cybersecurity and Infrastructure Security Agency
Communications	Cybersecurity and Infrastructure Security Agency
Critical Manufacturing	Cybersecurity and Infrastructure Security Agency
Dams	Cybersecurity and Infrastructure Security Agency
Defense Industrial Base	Department of Defense
Emergency Services	Cybersecurity and Infrastructure Security Agency
Energy	Department of Energy
Financial Services	Department of Treasury
Food and Agriculture	Department of Agriculture and Department of Health and Human Services
Government Facilities	General Services Administration
Healthcare and Public Health	Department of Health and Human Services
Information Technology	Cybersecurity and Infrastructure Security Agency
Nuclear Reactors, Materials, and Waste	Cybersecurity and Infrastructure Security Agency
Transportation Systems	Department of Transportation
Water and Wastewater Systems	Environmental Protection Agency

Infrastructure Resilience Planning Framework (IRPF)

November 2022 | Version 1.1

Infrastructure Development and Recovery Program - IDR@cisa.dhs.gov

Cyber Disruption Response Plan

Hawai‘i Office of Homeland Security

MARCH 2022 |

AUTHORITY AND ADOPTION LETTER

EXECUTIVE SIGNATORY PAGE

The most fundamental function of government is providing for the safety and welfare of the public. An effective Cyber Security program is essential to ensuring the state of Hawai'i fulfills this responsibility when our state is threatened or impacted by cyber disruption.

The State of Hawai'i ***Cyber Disruption Response Plan (CDRP)*** establishes the framework our State Government will use to organize and coordinate its response activities for a coordinated approach to responding to cyber disruptions that impact our state.

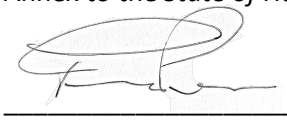
This CDRP, an Incident Annex to the State Emergency Operations Plan, outlines organizations, actions, and responsibilities of state and county departments and agencies and identifies how they will work together to ensure the state is prepared to execute a well-coordinated, timely and consistent cyber disruption response. It is intended to be a living document that evolves and improves as the outcomes of ongoing planning efforts, exercises, and real-world events are incorporated.

This plan is written in accordance with Hawai'i Revised Statutes (HRS) Chapters 128A (Homeland Security) and 128B (Cybersecurity) and applies to all state departments including agencies, offices, institutions of higher education, commissions, boards, and councils. This ***CDRP***/Annex does not direct the emergency operations of local governments, federal agencies, private sector, or non-governmental organizations. However, it does provide a reference for their response plans, procedures, and actions.

It is important to emphasize that responsibility for the initial response and management of an emergency rests with the affected entity(ies), to include local jurisdictions. The state's response supports state government efforts when additional resources are required or not available within the affected entity. This plan describes how those state resources will be activated, requested, and coordinated to complement response efforts.

This document is maintained by the Hawai'i State Office of Homeland Security (OHS) with input from state and county departments and agencies.

I hereby promulgate and adopt the State of Hawai'i ***Cyber Disruption Response Plan*** as an Incident Annex to the *State of Hawai'i Emergency Operations Plan***.**



_____

Frank J. Pace, Administrator
Office of Homeland Security
Hawai'i Department of Defense
MAR 2, 2022

RECORD OF APPROVAL

Approval #	Approval Date	Approval Authority	Type of Approval
2			
1			

RECORD OF CHANGES

Change Number	Date of Change	Page or Section Changed	Summary of Change	Authorization Signature	Date of Signature
1					
2					
3					
4					
5					
6					
7					

TABLE OF CONTENTS

1. INTRODUCTION

1.1 PURPOSE

In Hawai'i Revised Statutes (HRS) Chapter 128A (Homeland Security) the state legislature; finding existing and increasing possibility of attacks (defined to include cyber) of unprecedented size and destructiveness and to ensure adequate preparation to deal with such attacks; preserve the lives and property of the people of the State; and protect the public peace, health, and safety; created the Hawai'i State Office of Homeland Security (OHS). Chapter 128A outlines the OHS responsibilities to include preparing comprehensive plans and programs for homeland security. HRS Chapter 128B (Cybersecurity) Cybersecurity Coordinator were absorbed into the OHS when that position was abolished. Under these collective authorities, the OHS, in coordination with appropriate entities and individuals, develops, regularly updates, maintains, and exercises adaptable response plans to address cybersecurity risks, including significant cyber incidents (***disruptions***) contemplated in this ***Cyber Disruption Response Plan***.

The ***Presidential Policy Directive (PPD)-41: U.S. Cyber Incident Coordination*** set forth principles governing the Federal Government's response to any cyber incident, provide an architecture for coordinating the response to significant cyber incidents, and required DHS to develop a ***National Cyber Incident Response Plan (NCIRP)***. This ***CDRP*** follows the ***NCIRP*** concept as part of the broader National Preparedness System and establishes the framework for a whole-of-Nation[1] approach to responding to a cyber incident ***(disruption)*** in the State of Hawai'i. This whole-of-Nation concept focuses efforts and enables the full range of stakeholders—the private and nonprofit sectors (including private and public owners and operators of critical infrastructure), state and local governments, and the Federal Government—to participate as full partners in incident ***(disruption)*** response and both includes and strongly relies on public and private partnerships to address major cybersecurity risks.

Any organization with sensitive data can be attacked, regardless of size or sector. And as the threat landscape evolves and adversaries deploy tactics, techniques, and procedures, security professionals and stakeholders must also adapt their security plans. Depending on the situation, a targeted attack may involve the theft of source code, valuable intellectual property, negotiation data or general operational disruption. Companies and governments need to be prepared to identify, respond to, and mitigate a targeted attack with the same amount of effort that goes into implementing a disaster response or recovery plan.[2]

States are now developing disruption response plans to respond to a significant cyber incident — cyberattacks that "pose demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of

[1] The whole-of-Nation approach also encompasses a wide range of new and existing public and private partnerships to leverage as a platform in working towards managing cybersecurity threats and hazards to critical infrastructure.
[2] CrowdStrike Services. (undated). *You've Been Breached – Now What?: How to Respond to a Worst-Case Cyber Scenario.* Accessed September 10, 2021 at: WhitepaperIncidentResponse.pdf (crowdstrike.com)

[the public]."[3] These plans differ from incident response plans because they require multiple agencies to coordinate activities and implement traditional emergency management and homeland security operations. Like a Category 5 hurricane, states realize that they have a role in mitigating the impact of such a scenario and are solidifying those roles and responsibilities in cyber disruption response plans.[4]

1.2 SCOPE

This ***CDRP*** describes the framework for state cyber disruption response and short-term recovery coordination among multiple state, local, and federal agencies and private entities with critical computer information or operational systems or cyber response assets or capabilities. This plan provides a framework for a cyber response and short-term recovery, including the establishment of a Cyber Unified Coordination Group (C-UCG) and an outline of the C-UCG's roles and responsibilities in the coordination of rapid identification, information exchange, response, and short-term recovery and remediation to mitigate the damage caused by either a deliberate or unintentional significant cyber incident. Activities conducted pursuant to this ***CDRP*** are compliant with the National Incident Management System (NIMS) and take place within state and local planning and incident command structures, complement existing plans and procedures.

1.2.1 Policy

Procedures for utilization, control and use will incorporate and/or consider operational priorities that include, but are not limited to, the protection of life, public health and safety, property protection, environmental protection, restoration of essential utilities, restoration of essential program functions, and coordination as appropriate.

The governor or designee may authorize and direct the use of state resources to provide support and assistance to disruption handling efforts for internal and external organizations after consideration of both priority of need and cost.

In situations where an imminent threat exists to life safety, or an identified need for the protection of critical infrastructure and environment exists, priorities established within the ***Hawai'i Emergency Operations Plan (HI-EOP)*** take precedence over agency priorities.

1.2.2 Definitions

Asset response activities include furnishing technical assistance to affected entities, mitigating vulnerabilities, identifying additional at-risk entities, and assessing their risk to the same or similar vulnerabilities.

[3] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan*. Accessed September 10, 2021 at: National Cyber Incident Response Plan - December 2016 (cisa.gov)

[4] National Governor's Association. (2019, July). *Issue Brief: State Cyber Disruption Response Plans.* Accessed September 10, 2021 at: IssueBrief_MG.pdf (nga.org)

A ***cyber-attack*** is "an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity."[5] Cyber-attacks are intentional and can be carried out by individuals, organizations, or government entities. They range from unsophisticated attempts made by amateur hackers using existing computer scripts, to sophisticated attempts sponsored or carried out by international governments. There are many types of attacks in between these extremes. "Hacktivists" are individuals or groups who use hacking to promote their social or political ideology. Additionally, threat agents may use ransomware, malicious software designed to restrict access to a system or data until a sum of money is paid. Espionage and data theft could degrade public safety, expose the State or its counties to financial risk and the public to identity theft. In 2019, Hawai'i state victims of internet crimes lost over $9 million, mostly through fraud schemes.[6] Tactics used in cyber-attacks are always changing and becoming more sophisticated. The U.S. Department of National Intelligence's 2018 Worldwide Threat Assessment states that U.S. adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners.[7] The report goes on to say that while cyber-attack as a foreign policy tool has been mostly confined to low-level attacks, these state-sponsored actors have been testing more aggressive tactics in recent years. In 2016, the Department of Homeland Security stated that they were confident that Russia was responsible for hacking the Democratic National Committee (DNC) and leaking thousands of DNC emails during the presidential election.[8]

A ***cyber-crime*** is any type of illegal activity that takes place via digital means. Data theft is one of the most common types of cyber-crime, but cyber-crime also includes a wide range of malicious activity such as cyberbullying or planting worms or viruses. The top three crime types reported by victims in 2019 were phishing/vishing/smishing/pharming, non-payment/non-delivery, and extortion.[9]

A ***cyber incident*** is "an event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon." [10]

---

[5] Check Point Software Technologies LTD (undated). *What Is a Cyber Attack?* Accessed September 10, 2021 at: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/

[6] FBI Internet Crime Complaint Center data. (Undated). Accessed September 10, 2021 at: https://www.ic3.gov/Media/PDF/AnnualReport/2019State/StateReport.aspx#?s=14

[7] Coats, Daniel R. Office of the Director of National Intelligence. (2019, January). *Worldwide Threat Assessment of the US Intelligence Community.* Accessed September 10, 2021 at: https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

[8] U.S. Department of Homeland Security. (2016, October). *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security.* Accessed September 10, 2021 at: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

[9] U.S. Department of Homeland Security. (2020, February). *FBI Releases IC3 2019 Internet Crime Report*. Accessed at: https://us-cert.cisa.gov/ncas/current-activity/2020/02/12/fbi-releases-ic3-2019-internet-crime-report

[10] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan*. Accessed September 10, 2021 at: National Cyber Incident Response Plan - December 2016 (cisa.gov)

A ***denial-of-service*** attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.[11]

An ***Electromagnetic Pulse (EMP)*** is an intense burst of electromagnetic energy resulting from natural (e.g., solar storms) or human (e.g., nuclear or pulse-power device) sources. Both types can destroy or damage unshielded electrical and electronic equipment. Solar storms can induce extreme currents in wires, disrupting power lines, and causing wide-spread blackouts to the communication cables that support the internet.[12] There is still much we do not understand about how effective nuclear weapons are as EMP weapons, especially lower yield bombs that terrorists or small states would probably use. The scale and scope of damage caused by an EMP could vary considerably based on the type of device, and the altitude and latitude of the detonation. A nuclear device detonated at high altitudes (30-400 km) could generate an EMP with a radius of effects from hundreds to thousands of kilometers.[13] While it could disable electrical and electronic systems in general, it would pose the highest risk to electric power systems and long-haul communications.[14]

Indirect Effect. Other hazards or human error can have effects on digital networks and information. Power outages can create cyber disruptions. In 2006 many parts of Seattle lost power for days. Many individuals and small businesses had trouble powering computers and mobile devices. As computers become our primary tools for gathering information and communicating, their loss can endanger public safety and welfare. If the power goes out and fuel delivery to generator sites is impaired, bigger sites like communications hubs and data centers could go down causing disruption if they are not adequately backed up. Additionally, communications equipment often sits under high-powered sprinklers. If there was a fire in one of these buildings or a sprinkler head was knocked off, it could damage equipment and cause disruptions to communications. Human error can also play a role in cyber-related incidents. An unintentional release of sensitive digital information presents a potential threat to personal and financial security.

[11] U.S. Department of Homeland Security. (2019, November). *National Cyber Awareness* System. Accessed September 10, 2021 at: https://us-cert.cisa.gov/ncas/tips/ST04-015

[12] National Aeronautics and Space Administration. (2009, January). *NASA-Funded Study Reveals Hazards of Severe Space Weather.* Accessed September 10, 2021 at: https://www.nasa.gov/topics/solarsystem/features/spaceweather_hazard.html.

[13] U.S. Department of Energy. (2017, January). *U.S. Department of Energy Electromagnetic Pulse Resilience Action Plan*. Accessed September 10, 2021 at: https://www.energy.gov/sites/prod/files/2017/01/f34/DOE%20EMP%20Resilience%20Action%20Plan%20January%202017.pdf

[14] Ibid.

Intelligence support activities include information to better understand the cyber incident and existing targeted diplomatic, economic, or military capabilities to respond and share threat and mitigation information with other potential affected entities or responders.

Physical Damage. Cyber disruptions can also happen as secondary effects from other kinds of hazards. Earthquakes, floods, and fires can destroy computer and network equipment. Most of the time the effects are limited due to the availability of back-up systems and the ability to route networks around problem sites. Nevertheless, if a significant network node goes down the effects could be wide-spread and possibly prolonged. Communications can be disrupted by physical damage to copper or fiber cables, or radio equipment located on buildings. Damage to cables has accidentally occurred during construction or repaving projects, causing temporary internet and phone outages for thousands of customers.

A ***significant cyber incident*** is defined as a "a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."[15]

Threat response activities during a cyber incident include investigative, forensic, analytical, and mitigation activities; interdiction of a threat actor; and providing attribution that may lead to information sharing and operational synchronization with asset response activities.

1.2.3 Relationship to Other Plans

The ***Cyber Disruption Response Plan (CDRP)*** is an Annex to the ***HI-EOP*** which is the state's all-hazards plan that establishes the framework used to coordinate the state response to, and recovery from, emergencies and disasters. The ***CDRP*** Annex addresses unique planning, response, and short-term recovery requirements for cyber disruption (a significant cyber incident) but is not intended to duplicate or alter the response concepts outlined in the ***HI-EOP.***

Additionally, the ***Cyber Incident Response Plan (CIRP)*** is an Appendix to the State of Hawai'i ***CDRP***. The ***CIRP*** addresses unique planning and response requirements for a state Information Technology (IT) enterprise cyber incident but is not intended to duplicate or alter the response concepts outlined in this ***CDRP.***

[15] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan*. Accessed September 10, 2021 at: National Cyber Incident Response Plan - December 2016 (cisa.gov)

2. SITUATION AND ASSUMPTIONS

2.1 SITUATION OVERVIEW

Cyber incidents may take many forms:

- An organized attack;
- An uncontrolled exploit, such as a virus, worm, or Denial of Service which has a widespread impact on public safety;
- A natural disaster with significant cyber consequences;
- Other incidents causing extensive damage to critical infrastructure;
- Inadequate or improper IT infrastructure maintenance, security, and/or design.

In addition, an incident can be a "false positive" where no actual damage or danger is present, but an investigation is needed to reach that conclusion.

Cyber-attacks, cyber-crime, and unintentional incidents caused by natural disaster or human error can also lead to large scale or long-term disruption of service. The results of these events can lead to the loss of mission critical information, unavailability of information systems that support public sector internet, critical infrastructure, public health, economic institutions, and other organization that sustain and provide critical services to State Hawai'i residents and visitors. Cyber threats can endanger vital control systems for other infrastructure such as electricity generation, transmission, and distribution.

Information technology service providers within Hawai'i play a vital role in cyber incident response because the public sector provides the backbone for IT systems and are the most predominant owners/operators of the critical infrastructure and performers of critical functions that IT systems support. Federal, State, and local Government computer assets are all connected in varying degrees to privately administered critical communications infrastructure providers. It is essential that these providers be integrated into the coordination and decision-making processes in this ***CDRP.***

Cyber incidents have the potential to overwhelm or disable government and private sector resources. The computer networks utilized by State of Hawai'i government agencies and those that support critical infrastructure provide critical services, including those that support public safety and public health. Technical staff within organizations must keep up with current technologies as cyber threats change, and the training can be expensive. Redundancy must continue to be built into computer networks, and continuity of operations plans for all governmental and critical infrastructure organizations must be maintained and tested.

2.1.1 THREAT ANALYSIS

Because of the relative lack of cybersecurity expertise and their need to stay operational state and local governments have become a favored target of cybercriminals, especially ransomware operators, because small government agencies are more likely to pay to recover from a ransomware attack.[16]

Since 2017, attacks – which the report defines as targeted instances of intrusion, fraud, or damage by malicious cyber actors rather than discovery of insecure databases or accidental online leaks – rose an average of almost 50%, likely only a fraction of the true number.[17]

Ransomware is the main way municipal assets are attacked. What is more concerning than the growing number of attacks, however, is the increase in how much bad actors demand in ransom. Average ransom demands rose from a monthly average of $30,000 to nearly half a million dollars, with total monetary value of ransom demands reaching into the millions.[18]

Even when cities do not pay, the costs can be staggering. For instance, the 2019 ransomware attack on Baltimore cost the city more than $18 million in damages and remediation.[19]

Looking forward, a recent trends outlook highlighted eight trends anticipated for 2021:[20]

- Next-Generation Extortion and Evolution in Malware Business Models
- Supply Chain Attacks via Cloud-Hosted Development Environments
- AI, Evasion, and Theft
- Parcel and Shipping as Critical Infrastructure
- Mandated Contact Tracing Apps May Open Doors for Large-Scale Cyber Attacks
- Cybercriminals Will Likely Capitalize on Rapid U.S. Telehealth Adoption
- 5G to Expand the Attack Surface for Industrial IOT
- 5G to Increase Security Pressure on Mobile Hotspots

Hawaii's cyber security risk profile trends medium to high:

- **People:** There is increasing possibility of attacks that paralyze critical infrastructure sectors/facilities, creating far-reaching effects statewide, impacting most, if not all, of the population.
- **Property:** Damages can vary wildly but are most likely going to be localized. While statewide, risk to properties is minimized due to the state's archipelago nature, property impacts from

[16] DARKReading. (2020, June). *Local, State Governments Face Cybersecurity Crisis.* Accessed November 12, 2020 at: https://www.darkreading.com/attacks-breaches/local-state-governments-face-cybersecurity-crisis/d/d-id/1338010#:~:text=Already%2C%20government%2Dfocused%20companies%20have,state%20and%20local%20government%20clients.&text=In%202019%2C%20more%20than%20104,threat%20intelligence%20firm%20Recorded%20Future.

[17] BlueVoyant. (2020, August). *State and Local Government Security Report.* Accessed November 12, 2020 at: https://www.bluevoyant.com/state-and-local-gov-security-report

[18] Ibid.

[19] GCN. (2020, September). *Cyberattacks on state, local government up 50%.* Accessed November 12, 2020 at: https://gcn.com/articles/2020/09/04/cyberattacks-state-local-government-climbing.aspx.

[20] Booz-Allen-Hamilton. (2020). *2021 Cyber Threat Trends Outlook.* Accessed November 12, 2020 at: https://boozallen.com/content/dam/boozallen_site/ccg/pdf/publications/cyber-threat-trends-outlook-2021.pdf

cyber incidents is increasingly fluid across a broad attack surface implicating multiple sectors and/or multiple victims.

- **Environment:** Cyber intrusions and attacks can pose a significant pollution liability risk with potential to cause damage to human health and the environment from catastrophic spills, waste discharges, and air emissions. These events can cause fires, explosions and hazardous material releases that result in bodily injury, property damage, and environmental remediation.
- **Continuity / Operations:** A cyber-attack against State or county government or critical infrastructure that responsible responding organizations are dependent upon (i.e., electricity, communications, transportation) could completely cripple State and local government and/or state and county emergency management program operations until systems could be restored.

2.1.2 VULNERABILITY ANALYSIS

Based on analysis of FBI cyberattack data, states' who report to the National Governor's Association for spending on cybersecurity and how safe each state's election systems are, Hawai'i ranks at the top of those states at most risk of cyberattacks.[21] While that analysis was looking across all of the state and through the lens of election systems and not focused on the state IT enterprise, like other states in the nation, the State of Hawai'i continues to work to increase their cybersecurity posture with limited resources.

At the time of the writing of this plan, the Coronavirus Disease that appeared in 2019 (COVID-19) has dominated every state's leadership agenda for most of 2020 and 2021, and that is true for the State of Hawai'i IT enterprise. But even before, the enterprise was dealing with the ongoing struggle for adequate funding, challenges of cyber staffing, and ever-evolving cyber threats. COVID-19 acted as a major accelerant, increasing the urgency of efforts of critical importance.

Telework was already happening, but on a smaller scale. As of this writing, remote work is the dominant operating principle of state government. Additionally, there was more data to protect due to unprecedented demand for government services such as unemployment compensation and other digital services. Some of these changes are likely to become permanent, continuing to strain against the state's cybersecurity vulnerabilities:

- Lack of sufficient cybersecurity budget
- Inadequate cybersecurity staffing
- Legacy infrastructure and solutions to support emerging threats
- Lack of dedicated cybersecurity budget
- Inadequate availability of cybersecurity professionals

When looking more broadly, Hawaii's cyber security vulnerability profile trends medium to high:

[21] Security.org. (2019, August). *What States Are at Highest Risk for Cyberattacks.* Accessed November 12, 2020 at: https://www.security.org/resources/states-highest-risk-cyberattacks/.

- **People:** Depending on the type of attack and its target, vulnerable populations could be specific agencies/organizations or groups, but can just as readily encompass multiple sectors, critical functions, and create vulnerable populations with their impacts.
- **Property:** Industrial control systems such as water treatment facilities/pipelines and transportation systems are vulnerable to cyber-attack. All critical infrastructure sectors are (and increasingly so) vulnerable to ransomware attacks that can render systems inoperable temporarily or permanently, necessitating complete replacement.
- **Environment:** All ecosystems that have interface with cyber-reliant or cyber-enabled human infrastructure systems, including marine and air, carry the potential to sustain environmental impacts from and are vulnerable to cyber-attacks.
- **Continuity / Operations:** Plans calling for documentation and system backups provide minimal continuity for state/county and their emergency management programs without significant delay; however, these plans and this mitigation approach are not universal to all government organizations that have responsibilities in supporting emergency management and that inhibits those operations in the state. Additionally, operational effectiveness will be impacted more so should critical infrastructure sectors also experience direct or cascading impacts from a cyber incident.

In the national context, vulnerability for the State of Hawai'i also comes in the form of a significant partner and neighbor on the islands. The U.S. Department of Defense's (DoD's) U.S. Indo-Pacific Command (USINDOPACOM) Headquarters and all its supporting service component's headquarters on Oahu and has several other installations strewn amongst the island chain. This cluster of military capability is an attractive target for hostile nation-states and other actors. In the event of a cyber incident, both the U.S. military and the state government could face devastating disruption to their IT enterprises as well as other life-sustaining services.

2.2 ASSUMPTIONS

- Affected entities may not have operational situational awareness and/or control or be responsible for incident response activities based on applicable laws, statutes, and authorities.
- Notification to state agencies regarding cyber incidents will be carried out in accordance with this ***CDRP***.
- The ***CDRP*** is based on current Hawai'i Revised Statues; any further required/desired authorities or similar would require additional statues to be developed.
- Due to limits on situational awareness, activation the Emergency Operations Plan/Emergency Operations Center will be a decision point based on the nature and awareness of the extent of the disruption.
- There will not be sufficient cyber incident response capability at the affected entity or within the state.

- Mutual aid agreements and pre-scripted missions will be required to meet response requirements for a significant cyber incident.
- Affected entities will follow their relevant response plans, including consultation with any pre-arranged no cost retainer legal and breach consulting experts and cyber security and forensic analysis companies, to take appropriate actions such as terminating unauthorized access, minimizing damage, analyzing scope and depth of intrusion, and preservation evidence.
- The effects of a significant cyber incident may be widespread affecting multiple entities, both public and private, and have local and state impacts, for a period lasting beyond two weeks.
- Without help from residents, professionals, and private-sector organizations, the state government alone will not have the scale to improve the overall cybersecurity of Hawai‘i.

3. CONCEPT OF OPERATIONS

3.1 PREPARATION

Incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. Although the incident response team is not typically responsible for incident prevention, it is fundamental to the success of incident response programs.[22]

A significant cyber incident (e.g. Ransomware outbreak, Denial of Service attacks, etc.) may create effects of such magnitude against information systems, resources, and operations and across multiple entities simultaneously or near-simultaneously such that it may require the Governor to declare an emergency and activate the necessary resources to respond to and perform short-term recover to stem potential damage and/or loss of confidentiality, integrity, availability, reputation, and public trust.

Upon activation, all applicable National, State, local, interjurisdictional, and private sector significant cyber incident response organizations (or functional equivalent) should provide cooperation and coordination with the designated entities, affected agency(ies), and appointed officers in response and short-term recovery efforts. All parties should identify and prioritize the appropriate means to:

- Communicate securely and effectively with designated response/recovery entity members (e.g., situation/war room); contact information is crucial.
- Coordinate the use of response and short-term recovery resources (e.g., analysis tools, mitigation software, etc.) and personnel management.
- Track and monitor the incident response and short-term recovery activities (e.g., incident tracking/ticketing mechanisms, etc.) until closure.

3.2 DETECTION, ANALYSIS, AND NOTIFICATION

Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident. Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors. Different types of incidents merit different response strategies.[23]

3.2.1 Detection

Signs of an incident fall into one of two categories: precursors and indicators. A precursor is a sign that an incident may occur in the future. An indicator is a sign that an incident may have occurred or may

[22] National Institute of Standards and Technology. (2012, August). *Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology.* Accessed September 10, 2021 at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[23] Ibid

be occurring now. Most attacks do not have any identifiable or detectable precursors from the target's perspective. If precursors are detected, the organization may have an opportunity to prevent the incident by altering its security posture to save a target from attack. At a minimum, the organization could monitor activity involving the target more closely.[24]

3.2.1 Impact Analysis

Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis because of resource limitations. Instead, handling should be prioritized based on the relevant factors, such as:[25]

Functional Impact of the Incident. Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems. Incident handlers should consider how the incident will impact the existing functionality of the affected systems. Incident handlers should consider not only the current functional impact of the incident, but also the likely future functional impact of the incident if it is not immediately contained.

Information Impact of the Incident. Incidents may affect the confidentiality, integrity, and availability of the organization's information. Incident handlers should consider how this information exfiltration will impact the organization's overall mission. An incident that results in the exfiltration of sensitive information may also affect other organizations if any of the data pertained to a partner organization.

Recoverability from the Incident. The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident. In some instances, it is not possible to recover from an incident and it would not make sense to spend limited resources on an elongated incident handling cycle, unless that effort was directed at ensuring that a similar incident did not occur in the future. In other cases, an incident may require far more resources to handle than what an organization has available. Incident handlers should consider the effort necessary to recover from an incident and carefully weigh that against the value the recovery effort will create, and any requirements related to incident handling.

3.2.2 Notification and Activation

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber-attacks that damage computer systems can cause lasting harm to anyone engaged in

[24] National Institute of Standards and Technology. (2012, August). *Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology.* Accessed September 10, 2021 at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[25] Ibid

personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.[26]

A private sector entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery.[27]

When supporting affected entities, the Hawai'i State Government, and the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice.

When to Report

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Hawai'i State and Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact many victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

What to Report

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

[26] U.S. Department of Homeland Security. (Undated). *Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government*. Accessed October 28, 2021 at: https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf
[27] Ibid

How to Report

If there is an immediate threat to public health or safety, initial notice should always be to 911.

Private sector entities experiencing cyber incidents within the state of Hawai'i are encouraged to report to the Hawai'i State Fusion Center, local field offices of federal law enforcement agencies, their sector specific agency, and any of the applicable federal agencies listed section 4.3. The entity receiving the initial report will coordinate with other relevant state and federal stakeholders in responding to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation in addition to voluntarily reporting the incident as described above. The affected entity is responsible for internal and support partner notifications, alerts.

Key State Point of Contact:

Hawai'i State Fusion Center (HSFC)

HSFC: (808) 369-3589 or HSFC@hawaii.gov

Report suspected or confirmed cyber incidents, intrusions, or attacks, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.

Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity.

Report cyber-enabled crime, including digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.

Key Federal Points of Contact:

National Cybersecurity and Communications Integration Center (NCCIC)

NCCIC: (888) 282-0870 or NCCIC@hq.dhs.gov
United States Computer Emergency Readiness Team: http://www.us-cert.gov

Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.

Federal Bureau of Investigation (FBI)

FBI Field Office Cyber Task Forces: http://www.fbi.gov/contact-us/field
Internet Crime Complaint Center (IC3): http://www.ic3.gov

Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.

Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.

National Cyber Investigative Joint Task Force

NCIJTF CyWatch 24/7 Command Center: (855) 292-3937 or cywatch@ic.fbi.gov

Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.

United States Secret Service

Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs):
http://www.secretservice.gov/contact/field-offices

Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information.

United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI)

HSI Tip Line: 866-DHS-2-ICE (866-347-2423) or https://www.ice.gov/webform/hsi-tip-form
HSI Field Offices: https://www.ice.gov/contact/hsi
HSI Cyber Crimes Center: https://www.ice.gov/cyber-crimes

Report cyber-enabled crime, including digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.

United States Coast Guard (USCG)

USCG Sector Honolulu: 808-842-2600
National Response Center: 800-424-8802

Report, without delay, cyber incidents and suspicious activities impacting security and/or safety of maritime ports, vessels, and waterways.

COORDINATION OF PUBLIC INFORMATION. Reference the State Emergency Operations Plan for details regarding coordination of this element of notification concerning information to be shared publicly. Alert and warning are not mandatory; unless required by law, statute or regulatory directed. If required, the State of Hawai‘i through the C-UCG and related response mechanisms will coordinate with affected entities to assist with meeting this requirement.

ACTIVATION OF THE STATE EMERGENCY OPERATIONS CENTER (SEOC). The need to activate the State EOC is based on the scope, scale, and complexity of a threatening or occurring cyber incident. OHS will notify HSFC regarding notifications, alerts, and/or warnings to stakeholders, key-decision makers, and

executive officers. OHS will also provide advice and recommendations to the Homeland Security Advisor regarding the need or desire to stand up a C-UCG, which would also include incident notification to the State EOC.

Upon State EOC notification of a significant cyber incident, the level of SEOC activation will be determined by the Administrator of Emergency Management, Executive Officer, or Operations Section Chief in conjunction with the decision to activate a C-UCG.

3.3 INCIDENT HANDLING

3.3.1 Containment

Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early while handling each incident. Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident. Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly. Containment strategies vary based on the type of incident.[28]

Evidence Gathering and Handling - While the primary reason for gathering evidence during an incident by the affected entity is to resolve the incident, it may also be needed for legal proceedings, particularly when individual incidents are part of a larger ***significant cyber incident***. In such cases, it is important to clearly document how all evidence, including compromised systems, has been preserved. Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court. In addition, evidence should be always accounted for; whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature. A detailed log should be kept for all evidence.[29]

Identifying the Attacking Hosts - During incident handling, system owners and others sometimes want to or need to identify the attacking host or hosts. Although this information can be important, incident handlers in affected entities should generally stay focused on containment, eradication, and recovery. Identifying an attacking host can be a time-consuming and futile process that can prevent a team from achieving its primary goal—minimizing the operational impact.[30]

[28] National Institute of Standards and Technology. (2012, August). *Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology.* Accessed September 10, 2021 at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[29] Ibid.

[30] Ibid.

3.3.2 Eradication

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.[31]

3.3.3 Recovery

In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security. Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner.[32]

For large-scale incidents, recovery may take months; the intent of the early phases should be to increase the overall security with relatively quick (days to weeks) high value changes to prevent future incidents. The later phases should focus on longer-term changes (e.g., infrastructure changes) and ongoing work to keep the enterprise as secure as possible.[33]

3.4 POST-INCIDENT ACTIVITY

One of the most important parts of incident response is also the most often omitted: learning and improving. Each significant incident response must enable evolution that reflects new threats, improved technology, and lessons learned. To this objective, the C-UCG will coordinate and host a "lessons learned" meeting with all involved parties after a significant cyber incident. The meeting should be held within several days of the end of the significant cyber incident. Questions to be answered in the meeting include:

- Exactly what happened, and at what times?
- How well did responding organizations and their staff perform in dealing with the incident?
- Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the organizations do differently the next time a similar incident occurs?

[31] Ibid.
[32] National Institute of Standards and Technology. (2012, August). *Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology.* Accessed September 10, 2021 at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
[33] Ibid.

- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

4. ROLES AND RESPONSIBILITES

4.1 HAWAIʻI STATE GOVERNMENT

4.1.1 STATE DEPARTMENT OF DEFENSE

4.1.1.1 OFFICE OF HOMELAND SECURITY

- Ensure that it has the standing capacity to execute its role in cyber incident response.
- Establish enhanced coordination procedures to prepare for significant cyber incidents that exceed its standing capacity, consisting of:
    - Dedicated leadership,
    - Supporting personnel,
    - Available facilities (physical and communications),
    - Internal processes enabling it to manage a significant cyber incident under demands that would exceed its capacity to coordinate under normal operating conditions.
- Identify the appropriate pathways for communicating with other state, local, and federal agencies during a significant cyber incident, including the relevant agency points-of-contact, and for notifying the State Homeland Security Advisor that enhanced coordination procedures were activated or initiated.
- Highlight internal communications and decision-making processes that are consistent with effective incident coordination.
- Outline processes for maintaining these procedures.
- In addition, OHS' enhanced coordination procedures will identify the agency's processes and existing capabilities to coordinate cyber incident response activities in a manner consistent with PPD-41.
- Maintain capacity and capability to obtain and maintain clearances and accesses to facilitate the quick sharing of information.
- Develop/update sector-specific procedures, as needed and in consultation with the sector(s), for enhanced coordination to support response to a significant cyber incident.
- Serve as state coordination point for cognizant federal entities.
- Advise the Governor on the need to declare a state emergency or request federal assistance.

4.1.1.1.1 THROUGH THE HSFC:

- Collect, analyze, and disseminate intelligence information.
- Conduct threat and risk analyses.
- Assist law enforcement as appropriate.
- Maintain liaison with the State EOC upon activation.

4.1.1.2 NATIONAL GUARD

The Hawai‘i National Guard (HING) is comprised of the Hawai‘i Army National Guard (HIARNG) and Hawai‘i Air National Guard (HIANG), with personnel across the State.

Hawai‘i Army National Guard - The HIARNG has a Defensive Cyber Operations Element (DCO-E) that may be deployable for state cyber disruption response. The DCO-E is primarily responsible for cybersecurity, information assurance and internal defense measures on the Department of Defense Information Network- National Guard (DoDIN-A NG) in a Title 32 U.S. Code (Title 32) status. Upon request for support, and with the approval of the Governor and Adjutant General, the HING DCO-E may also provide support for non-DoD mission partners in a State Active Duty (SAD) status. In certain circumstances, the DCO-E may be activated under Title 10 U.S. Code (Active Duty) status to meet immediate incident response needs.

Hawai‘i Air National Guard - The HIANG has several cyber Mission Defense Teams (MDTs) whose primary purpose is cyber defense of tasked DoD mission systems in Title 32 status. Upon request for support, and with the approval of the Governor and Adjutant General, HING MDT personnel may also provide support for non-DoD mission partners in a SAD status.

The HING also maintains units tasked with traditional information technology support who may also be available to support vulnerability assessment and cyber disruption recover efforts when in SAD status.

4.1.1.2.1 CAPABILITIES

Between the DCO-E and MDT, the HING may possess the capability to perform:

- Network security and vulnerability assessments
- Network Analysis
- Host-based Analysis
- Assessment and Detection
- Containment, Eradication, and Recovery support
- Collection and analysis of intrusion artifacts to enable mitigation efforts
- Cyber incident triage
- Threat data correlation to provide increased situational awareness

4.1.1.2.2 RESPONSE & RESPONSIBILITIES

All requests for HING support are thru State Emergency Support Function (SESF) Annex #20- Military Support, State of Hawai‘i Emergency Operations Plan (HI-EOP). In addition to responsibilities outlined in the HI-EOP, in a significant cyber incident (disruption) the HING:

- May assist in the analysis of incident information, development of situational awareness, and technical assistance to prevent, protect, respond to, recover from, and mitigate the effects of a cyber incident.
- May activate for external response assets upon request and gubernatorial approval.
- May provide cyber incident response, as directed by the governor and Adjutant General, regardless of scope or customer type.

- May provide initial outreach, liaison duties, or on-site assistance to critical infrastructure providers.
- May provide supplemental incident response personnel to help manage the incident and relieve personnel/reduce staff fatigue.
- May support State of Hawai'i Office of Homeland Security in the cyber threat information sharing mission.

4.1.1.2.3 AUTHORITIES AND AGREEMENTS

In December 2019, the Hawai'i Office of Enterprise Technology Services (ETS) signed a Memorandum of Understanding with the Hawai'i National Guard.

The Parties agreed "to collaborate to increase their capacity and capability to defend against and respond to cyberattacks perpetrated against the citizens, public and private institutions, and the critical infrastructure of the State of Hawai'i and the United States. The Parties agree to jointly conduct training exercises, cybersecurity threat and defense assessments, computer network defense operations, and incident response activities to protect the public health, welfare, and safety of Hawaii's citizens."

4.1.1.2.4 LIMITATIONS

HING members are not authorized to conduct intelligence activities, including foreign intelligence and counterintelligence, while operating under Title 32 or State Active Duty. HING personnel in State Active Duty are prohibited from accessing their federal security clearances without a federal sponsor. In consultation with HING legal representatives, the HING may be authorized to conduct shared situational awareness and information sharing activities in supporting of a state cyber disruption response.

4.1.1.3 EMERGENCY MANAGEMENT AGENCY

The Hawai`i Emergency Management Agency (HI-EMA) is established as the state emergency management agency by HRS 127A-3(a). HI-EMA maintains a comprehensive, coordinated, and cooperative emergency management program for the State, coordinating its activities with county emergency management agencies, federal agencies involved in emergency management, state departments and agencies, other states, the private sector, and non-governmental organizations (NGOs).

During a Cyber Disruption:

- Provide overall coordination for the state's response and recovery activities to any consequence management activities for physical effects related to the significant cyber incident, including activating the SEOC and SERT, provisioning resources requested by affected counties and state agencies and, when applicable, utilizing federal support. As appropriate, HIEMA's operation coordination will conform to the existing EOP processes.
- Advise the Governor on the need to declare a state emergency or request federal aid.

- At the direction of the Governor's office and in coordination with the Department of Attorney General, prepare state disaster proclamations and Presidential disaster requests for the Governor's signature.
- Coordinate requests for out-of-state mutual aid through the Emergency Management Assistance Compact (EMAC).

4.1.2 ATTORNEY GENERAL'S OFFICE

- Coordinate with appropriate prosecuting authorities for the prosecution of criminal cases brought by the state.

4.2 AFFECTED ENTITY(IES)

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber incidents that damage computer systems can cause lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by all levels of governments, businesses, consumers, and all other users of the Internet. An entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents.

When supporting affected entities, the various agencies of the Federal, State, and Local Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities to minimize impacts to assets/systems, reduce their vulnerabilities, and bring malicious actors to justice.

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the State and Federal Government. Accordingly, all victims are encouraged to report all cyber incidents as detailed in Section 3.2.2 Notification and Activation.

4.3 FEDERAL GOVERNMENT LINES OF EFFORT

Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: **Threat Response** and **Asset Response**. Irrespective of the type of incident or its corresponding response, Federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.[34]

The 2016 Presidential Policy Directive (PPD) 41, United States Cyber Incident Coordination articulates the principles governing the U.S. Federal Government's response to any cyber incident and, for

[34] U.S. Department of Homeland Security. (Undated). *Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government*. Accessed October 28, 2021 at: https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf

significant cyber incidents, establishes lead federal agencies and an architecture for coordinating the broader Federal Government response. The Federal Government has three lines of effort in cyber incident response. No single agency possesses all the authorities, capabilities, and expertise to deal unilaterally with a significant cyber incident.

Asset response efforts involve furnishing technical assistance to affected entities to help them recover from the incident. The Department of Homeland Security (DHS), through the National Cybersecurity and Communications Integration Center (NCCIC), is the lead federal agency for asset response activities for significant cyber incidents. Such activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery.[35]

Threat response efforts involve the investigation of the crime. The Department of Justice (DOJ), through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF), is the lead federal agency for threat response activities for significant cyber incidents. Such activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.[36]

Threat and asset responders will share some responsibilities and activities, which may include communicating with affected entities to understand the nature of the cyber incident; providing guidance to affected entities on available Federal resources and capabilities; promptly disseminating through appropriate channels intelligence and information learned during the response; and facilitating information sharing and operational coordination with other Federal Government entities.[37]

Intelligence support and related activities are coordinated by the Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, as the Federal lead agency for intelligence support and related activities. Such activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.[38]

[35] The White House. (2016, July). *Presidential Policy Directive – United States Cyber Incident Coordination.* Accessed September 13, 2021 at: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
[36] Ibid.
[37] Ibid.
[38] Ibid.

5. DIRECTION, CONTROL, AND COORDINATION

Any agency receiving initial reporting of a significant cyber incident will coordinate with all other relevant state, local, and federal stakeholders in responding to the incident, including determining whether to establish a Cyber Unified Coordination Group (UCG) to coordinate the response to the significant cyber incident.

5.1.1 State Cyber Unified Coordination Group

Formation. A Cyber Unified Coordination Group (C-UCG) will be formed and activated only in the event of a significant cyber incident and will be incident specific. A C-UCG may be formed by any of the following processes:

- At the direction of the Governor or the State Homeland Security Advisor;
- When two or more state or state and local agencies request its formation based on their assessment of the cyber incident against the severity schema; and or
- When a significant cyber incident affects critical infrastructure owners and operators identified by the Office of Homeland Security for which a cyber incident could reasonably result in catastrophic state, regional, or national effects on public health or safety, economic security, or national security.

Dissolution. A C-UCG will dissolve when enhanced coordination procedures for threat and asset response are no longer required or the authorities, capabilities, or resources of more than one state/local agency are no longer required to manage the remaining facets of the state response to an incident.

Responsibilities. To promote unity of effort in response to a significant cyber incident, a C-UCG will:

- Coordinate the cyber incident response in a manner consistent with the principles described in PPD-41;
- Ensure all appropriate State, local, and Federal agencies are incorporated into the incident response;
- Coordinate the development and execution of response and recovery tasks, priorities, and planning efforts, including international and cross-sector outreach, necessary to respond appropriately to the incident and to speed recovery;
- Facilitate the rapid and appropriate sharing of information and intelligence among C-UCG participants on the incident response and recovery activities;
- Coordinate consistent, accurate, and appropriate communications regarding the incident to affected parties and stakeholders, including the public as appropriate; and

- For incidents that include cyber and physical effects, form a combined UCG with the lead State, local, and Federal agencies or with any UCG established to manage the physical effects of the incident under the National Response Framework developed pursuant to PPD-8 on National Preparedness.

A C-UCG shall operate in a manner that is consistent with the need to protect intelligence and law enforcement sources, methods, operations, and investigations, the privacy of individuals, and sensitive private sector information.

The C-UCG will promptly coordinate with the State Attorney General, county Corporation Counsel, DOJ, general counsel from DHS, regulators, and other relevant state and federal agencies' attorneys about pertinent legal issues as they are identified to quickly consider and coordinate them with appropriate nongovernmental entities, as necessary.

Participation. In response to a significant cyber incident that includes the need to engage in consequence management activities for physical effects related to the incident, the State Government establishes two lead agencies:

- OHS is the lead agency for coordinating asset and threat response and intelligence support during a significant cyber incident.
- HI-EMA is the lead agency for coordinating response to any consequence management activities for physical effects related to the significant cyber incident.

OHS will administer and manage the state's incident handling efforts and coordinate as appropriate with whole community partners.

Upon implementation of the ***HI-EOP*** and activation of the State EOC, the Director of Emergency Management or designee will establish operational command, coordination of state resources and support organizations required for consequence management in accordance with the ***HI-EOP***.

The HI-EMA will manage and utilize the State EOC and coordinate with OHS to receive and disseminate information and intelligence, establish common strategic priorities and operating picture, and prioritize short-, intermediate- and long-term activities among the relevant organizations.

When a Cyber UCG is established, in addition to the two state lead agencies, OHS and HI-EMA, the Cyber UCG will also include relevant state and/or local coordinating agencies if the cyber incident affects or is likely to affect sectors they have coordinating authority/responsibility for, as well as other state/local cybersecurity centers, as deemed necessary per the specific significant cyber incident.

Like government participation, private sector involvement in a C-UCG will be limited to organizations with significant responsibility, jurisdiction, capability, or authority for response for that specific incident, which may not always include all organizations contributing resources to the response. Private Sector Cyber UCG participation will be voluntary, and participants should be from organizations which can determine the incident priorities for each operational period and approve an Incident Action

Plan, to include commitment of their organizations' resources to support execution of the Incident Action Plan. Per the Guiding Principles in PPD-41, out of respect for an affected entities' privacy and sensitive private sector information, the State Government will coordinate with the affected entity on the approach of wider incident dissemination for that incident. C-UCG participants will be expanded or contracted as the situation changes during that incident response.

Regardless of specific participant composition, a C-UCG shall operate in a manner that is consistent with the need to protect intelligence and law enforcement sources, methods, operations, and investigations, the privacy of individuals, and sensitive and protected private sector information.

6. PLAN DEVELOPMENT AND MAINTENANCE

This ***CDRP*** is developed with input from federal, state, non-governmental and private sector entities that will support a state IT enterprise cyber incident.

The OHS is responsible for coordinating all revisions to this Plan. Maintenance responsibilities include:

- Maintaining a plan review schedule.
- Reviewing all plan components and proposed changes for consistency.
- Obtaining approvals for changes from the appropriate approving authority.
- Ensuring notifications of approved changes are made and maintaining a record of changes.
- Coordinating changes through with ETS to synchronize with the ***CIRP*** and to ensure consistency with the ***HI-EOP***.

Review Cycle. OHS will complete periodic updates of this plan no less than every two years. Updates may be initiated to address any of the following:

- Minor administrative revisions needed to update terminology, titles, or agency names.
- Ensure risk and vulnerability analysis, planning assumptions and situation reflect current realities.
- Address relevant changes in federal or state laws, policies, structures, capabilities or other changes to emergency management standards or best practices.
- Incorporate substantive lessons learned from exercises, incident analysis or program evaluations.

7. AUTHORITIES AND REFERENCES

7.1 STATE LAWS, REGULATIONS AND DIRECTIVES

1. ***Hawai'i Revised Statutes (HRS) Chapter 128A.*** Homeland Security.
2. ***Hawai'i Revised Statutes (HRS) Chapter 128B.*** Cybersecurity.
3. ***Hawai'i Revised Statutes (HRS) Chapter 487N.*** Security Breach of Personal Information.
4. ***Hawai'i Revised Statutes (HRS) Chapter 127A.*** Emergency Management.

7.2 FEDERAL LAWS, REGULATIONS AND DIRECTIVES

1. ***Cybersecurity and Infrastructure Security Agency Act of 2018.*** Elevated the mission of the former National Protection and Programs Directorate within DHS and established the Cybersecurity and Infrastructure Security Agency (CISA).
2. ***U.S. Department of Energy Electromagnetic Pulse Resilience Action Plan, January 2017.*** In response to increased concern about the potential impacts to the electric grid from an electromagnetic pulse (EMP) the U.S. Department of Energy developed an EMP resilience strategy in coordination with the electric power industry. This Action Plan is structured to address each of the five strategic goals defined in that Joint Strategy and describes a series of actions for each goal.
3. ***National Cyber Incident Response Plan, December 2016.*** Recognized that the frequency of cyber incidents is increasing, and the trend is unlikely to be reversed anytime soon. It also acknowledged that the most significant of these incidents necessitate deliberative planning, coordination, and exercising of response activities.
4. ***Cybersecurity Act of 2015.*** Legislation that allows companies in the U.S. to share personal information related to cybersecurity with the government. The government could use this information as evidence to prosecute crimes.
5. ***Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, February 2013.*** This directive establishes national policy on critical infrastructure security and resilience. This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, as well as enhances overall coordination and collaboration.
6. ***National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience, 2013.*** This plan describes a national unity of effort to achieve critical infrastructure security and resilience. Based on the guidance in the National Plan, the partnership will establish and pursue a set of mutual goals and national priorities and employ common structures and mechanisms that facilitate information sharing and collaborative problem solving.
7. ***Health Insurance Portability and Accountability Act (HIPAA) of 1996.*** Under HIPAA, protected health information is individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations (PHI healthcare business uses).

8. ***Gramm-Leach-Bliley Act (GLBA) of 1999.*** The GLBA requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

7.3 REFERENCES

1. *State of Hawai'i Cyber Incident Response Plan (CIRP), March 2022.*
2. *Cybersecurity Incident & Vulnerability Response Playbooks,* November 2021
3. *FBI Releases IC3 2019 Internet Crime Report,* February 2020.
4. BlueVoyant - *State and Local Government Security Report,* August 2020.
5. Booz-Allen-Hamilton - *2021 Cyber Threat Trends Outlook,* 2020.
6. DARKReading - *Local, State Governments Face Cybersecurity Crisis,* June 2020.
7. GCN - *Cyberattacks on state, local government up 50%,* September 2020.
8. *Worldwide Threat Assessment of the US Intelligence Community,* January 2019.
9. *National Cyber Awareness System*, November 2019.
10. *State of Hawai'i Emergency Operations Plan (EOP),* November 2019.
11. Security.org - *What States Are at Highest Risk for Cyberattacks,* August 2019.
12. National Governor's Association - *Issue Brief: State Cyber Disruption Response Plans,* July 2019.
13. *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security,* October 2016.
14. *Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology,* August 2012.
15. *NASA-Funded Study Reveals Hazards of Severe Space Weather,* January 2009.
16. CrowdStrike Services - *You've Been Breached – Now What?: How to Respond to a Worst-Case Cyber Scenario,* undated.
17. Check Point Software Technologies LTD - *What Is A Cyber Attack?,* undated.

8. ATTACHMENTS

Attachment 1 – Acronyms
Attachment 2 – Checklist of Major Steps for Disruption Response and Handling
Attachment 3 – Model Cyber Incident Response Plan
Attachment 4 – Cyber Incident Severity Schema/National Response Coordination Center Activation Crosswalk
Attachment 5 – Core Capabilities and Critical Tasks
Attachment 6 – Guidance on Reporting a Cyber Disruption
Attachment 7 – Threat Levels and Anticipated Response
Attachment 8 – Communications Checklists

ABBREVIATIONS AND ACRONYMS

The following is a list of some of the common abbreviations and acronyms in this plan:

AI	Artificial Intelligence
C-UCG	Cyber Unified Command Group
CDRP	Cyber Disruption Response Plan
CIRP	Cyber Incident Response Plan
CISA	Cybersecurity and Infrastructure Security Agency
COVID-19	Coronavirus Disease 2019
DCO-E	Defensive Cyber Operations Element
DHS	Department of Homeland Security
DNC	Democratic National Committee
DoD	Department of Defense
DoDIN-A NG	Department of Defense Information Network- National Guard
DOJ	Department of Justice
ECTF	Electronic Crimes Task Force
EMP	Electromagnetic Pulse
EOC	Emergency Operations Center
ETS	Office of Enterprise Technology Services
FBI	Federal Bureau of Investigation
GLBA	Gramm-Leach-Bliley Act
HI-EOP	Hawai‘i Emergency Operations Plan
HIANG	Hawai‘i Air National Guard
HIARNG	Hawai‘i Army National Guard
HING	Hawai‘i National Guard
HIPAA	Health Insurance Portability and Accountability Act
HRS	Hawai‘i Revised Statutes
HSFC	Hawai‘i State Fusion Center
HSI	Homeland Security Investigations
ICE	Immigration and Customs Enforcement
IOT	Internet of Things
IT	Information Technology
MDT	Mission Defense Team
NCCIC	National Cybersecurity and Communications Integration Center
NCIJTF	National Cyber Investigative Joint Task Force
NCIRP	National Cyber Incident Response Plan
OHS	Office of Homeland Security
PPD	Presidential Policy Directive
SAD	State Active Duty

SESF	State Emergency Support Function
SOP	Standard Operating Procedure
USCG	United States Coast Guard
USINDOPACOM	United States Indo-Pacific Command

CHECKLIST OF MAJOR STEPS FOR SIGNIFICANT INCIDENT RESPONSE AND HANDLING

	Action	Completed
	Detection and Analysis	
1.	Determine whether and incident has occurred.	
1.1	Analyze the precursors and indicators.	
1.2	Look for correlating information.	
1.3	Perform research (e.g., search engines, knowledge base).	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence.	
2.	Prioritize handling of the incident based on the relevant factors (e.g., functional impact, information impact, recoverability effort, etc.).	
3.	Report the incident to the appropriate internal personnel and external organizations.	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence.	
5.	Contain the incident.	
6.	Eradicate the incident.	
6.1	Identify and mitigate all vulnerabilities that were exploited.	
6.2	Remove malware, inappropriate materials, and other components.	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them.	
7.	Recover from the incident.	
7.1	Return affected systems to an operationally ready state.	
7.2	Confirm that affected systems are functioning normally.	
7.3	If necessary, implement additional monitoring to look for future related activity.	
	Post-Incident Activity	
8.	Create a follow-up report.	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise).	

Source: NIST Special Publication 800-61, revision 2

MODEL CYBER INCIDENT RESPONSE PLAN

Public and private sector entities should consider creating an entity-specific operational cyber incident response plan to further organize and coordinate their efforts in response to cyber incidents. Each organization should consider a plan that meets its unique requirements and relates to the organization's mission, size, structure, and functions.

The National Institute of Standards and Technology Special Publication 800-61 (revision 2)[1] outlines several elements to consider when developing a cyber incident response plan. Each plan should be tailored and prioritized to meet the needs of the organization and adhere to current information sharing and reporting requirements, guidelines, and procedures, where they exist. As appropriate, public, and private sector entities are encouraged to collaborate in the development of cyber incident response plans to promote shared situational awareness, information sharing, and acknowledge sector, technical, and geographical interdependences.

The elements below serve as a starting point of important criteria to build upon for creating a cyber incident response plan:[2]

- Mission
- Strategies and goals
- Organizational approach to incident response
- Risk assessments
- Cyber Incident Scoring System/Criteria[3]
- Incident reporting and handling requirements
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization
- Communications with outside parties, such as:
    - Customers, constituents, and media
    - Software and support vendors
    - Law enforcement agencies
    - Incident responders

[1] National Institute of Standards and Technology. (2012, August). SP 800-61: Computer Incident Handling Guide, Revision 2. Accessed November 3, 2021 at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[2] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan, Annex C*. Accessed September 10, 2021 at: National Cyber Incident Response Plan - December 2016 (cisa.gov)

[3] The National Cybersecurity and Communications Integration Center Cyber Incident Scoring System could be used as a basis for an organizations operations center to assist in the internal elevation of a particular incident. https://www.us-cert.gov/NCCIC-Cyber-Incident-ScoringSystem.

  - Internet service providers
  - Critical infrastructure sector partners
- Roles and responsibilities (preparation, response, recovery)
  - State Fusion Center
  - Emergency Operations Center
  - Local, regional, state, tribal, and territorial government
  - Private sector
  - Private citizens
- A training and exercise plan for coordinating resources with the community
- Plan maintenance schedule/process.

CYBER INCIDENT SEVERITY SCHEMA / NATIONAL RESPONSE COORDINATION CENTER ACTIVATION CROSSWALK

When incidents impact the cyber and/or physical environment(s), certain decisions and activities require coordination in order to respond in the most appropriate manner. The graphic below compares the Cyber Incident Severity Schema released in Presidential Policy Directive 41: United States Cyber Incident Coordination and the Department of Homeland Security National Response Coordination Center Activation Scale when comparing response levels for cyber and physical incidents.

Description	Disaster Level	Cyber Incident Severity	Description	Observed Actions
Due to its severity, size, location, actual or potential impact on public health, welfare, and infrastructure it requires an extreme amount of federal assistance for response and recovery efforts for which the capabilities to support do not exist at any level of government.	Level 1	Level 5 *Emergency*	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens.	Effect
Requires elevated coordination among federal and SLTT governments due to moderate levels and breadth of damage. Significant involvement of FEMA and other federal agencies.	Level 2	Level 4 *Severe*	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	Presence
		Level 3 *High*	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
Requires coordination among federal and SLTT governments due to minor to average levels and breadth of damage. Typically, this is primarily a recovery effort with minimal response requirements.	Level 3	Level 2 *Medium*	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Engagement
		Level 1 *Low*	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
No event or incident anticipated. This includes routine watch and warning activities.	Level 4	Level 0	Unsubstantiated or inconsequential event.	Steady State

CORE CAPABILITIES AND CRITICAL TASKS

Each core capability identified in the National Cyber Incident Response Plan (NCIRP) has critical tasks that facilitate capability execution. These critical tasks are tasks that are essential to achieving the desired outcome of the capability. Critical tasks inform mission objectives, which allow planners to identify resourcing and sourcing requirements prior to an incident. The chart below describes each core capability and identifies critical tasks associated with each capability.

1. Access Control and Identity Verification Description: Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems. Also referred to as Authentication and Authorization.
Critical Tasks: • Verify identity to authorize, grant, or deny access to cyber assets, networks, applications, and systems that could be exploited to do harm. • Control and limit access to critical locations and systems to authorized individuals carrying out legitimate activities. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Perform audit activities to verify and validate security mechanisms are performing as intended. • Conduct training to ensure staff-wide adherence to access control authorizations.
2. Cybersecurity Description: Protect (and, if needed, restore) computer networks, electronic communications systems, information, and services from damage, unauthorized use, and exploitation. More commonly referred to as computer network defense, these activities ensure the security, reliability, confidentiality, integrity, and availability of critical information, records, and communications systems and services through collaborative initiatives and efforts.
Critical Tasks: • Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that could be exploited. • Secure, to the extent possible, public, and private networks and critical infrastructure (e.g., communication, financial, electricity sub-sector, water, and transportation systems), based on vulnerability results from risk assessment, mitigation, and incident response capabilities. • Create resilient cyber systems that allow for the uninterrupted continuation of essential functions. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.
3. Forensics and Attribution Description: Forensic investigations and efforts to provide attribution for an incident are complementary functions that often occur in parallel during a significant cyber incident.
Critical Tasks: • Retrieve digital media and data network security and activity logs. • Conduct digital evidence analysis, and respecting chain of custody rules. • Conduct physical evidence collections, analysis adhere to rules of evidence collection as necessary. • Assess capabilities of likely threat actors(s). • Leverage the work of incident responders and technical attribution assets to identify malicious cyber actor(s). • Interview witnesses, potential associates, and/or perpetrators if possible.

• Apply confidence levels to attribution assignments. • Include suitable inclusion and limitation information for sharing products in attribution elements guidance. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Perform audit activities to verify and validate security mechanisms are performed as intended.
4. Infrastructure Systems Description: Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity.
Critical Tasks: • Maintain a comprehensive understanding of the needs for the safe operation of control systems. • Stabilize and regain control of infrastructure. • Increase network isolation to reduce the risk of a malicious cyber activity propagating more widely across the enterprise or among interconnected entities. • Stabilize infrastructure within those entities that may be affected by cascading effects of the cyber incident. • Facilitate the restoration and sustainment of essential services (public and private) to maintain community functionality. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Maintain up-to-date data knowledge of applicable emerging and existing security research, development, and solutions.
5. Intelligence and Information Sharing Description: Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats of malicious cyber activity to the United States, its people, property, or interests. Intelligence and information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as necessary.
Critical Tasks: • Monitor, analyze, and assess the positive and negative impacts of changes in the operating environment as it pertains to cyber vulnerabilities and threats. • Share analysis results through participation in the routine exchange of security information— including threat assessments, alerts, threat indications and warnings, and advisories—among partners. • Confirm intelligence and information sharing requirements for cybersecurity stakeholders. • Develop or identify and provide access to mechanisms and procedures for confidential intelligence and information sharing between the private sector and government cybersecurity partners.42 • Use intelligence processes to produce and deliver relevant, timely, accessible, and actionable intelligence and information products to others as applicable, to include critical infrastructure participants and partners with roles in physical response efforts. • Share actionable cyber threat information with SLTT and international governments and private sectors to promote shared situational awareness. • Enable collaboration via online networks that are accessible to all participants. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
6. Interdiction and Disruption Description: Delay, divert, intercept, halt, apprehend, or secure threats related to malicious cyber activity.
Critical Tasks: • Deter malicious cyber activity within the United States, its territories, and abroad. • Interdict persons associated with a potential cyber threat or act.

• Deploy assets to interdict, deter, or disrupt cyber threats from reaching potential target(s). • Leverage law enforcement and intelligence assets to identify, track, investigate, and disrupt malicious actors threatening the security of the Nation's public and private information systems. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.
7. Logistics and Supply Chain Management Description: Facilitate and assist with delivery of essential commodities, equipment, and services to include the sustainment of responders in support of responses to systems and networks impacted by malicious cyber activity. Synchronize logistics capabilities and enable the restoration of impacted supply chains.
Critical Tasks: • Identify and catalog resources needed for response, prior to mobilization. • Mobilize and deliver governmental, nongovernmental, and private sector resources to stabilize the incident and integrate response and recovery efforts, to include moving and delivering resources and services to meet the needs of those impacted by a cyber incident. • Facilitate and assist delivery of critical infrastructure components to rapid response and restoration of cyber systems. • Enhance public and private resource and services support for impacted critical infrastructure entities. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Apply supply chain assurance principles and knowledge within all critical tasks identified above.
8. Operational Communications Description: Ensure the capacity for timely communications in support of security, situational awareness, and operations, by any and all means available, among and between entities affected by the malicious cyber activity and all responders.
Critical Tasks: • Ensure the capacity to communicate with both the cyber incident response community and the affected entity. • Establish interoperable and redundant voice, data, and broader communications pathways between SLTT, particularly state fusion centers, federal, and private sector cyber incident responders. • Facilitate establishment of quickly formed ad hoc voice and data networks on a local and regional basis so critical infrastructure entities can coordinate activities even if Internet services fail. • Coordinate with any UCG (or entity) established to manage physical (or non-cyber) effects of an incident. Ensure availability of appropriate secure distributed and scalable incident response communication capabilities including out-of-band communications mechanisms where traditional communications and/or systems are compromised. Adhere to appropriate mechanisms for safeguarding sensitive and classified information private sector personnel should obtain the necessary clearances and accesses to facilitate the quick sharing of information. • Protect individual privacy, civil rights, and civil liberties. • Cyber threat information also is conducted through automated indicator sharing using established formats such as Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information (STIX/TAXII).43 • Perform red team activities to verify and validate that forensics and attribution capabilities are performing as intended and have adequate visibility
9. Operational Coordination Description: Establish and maintain a unified and coordinated operational structure and process that appropriately integrate all critical stakeholders and support execution of core capabilities.
Critical Tasks:

• Mobilize all critical resources and establish coordination structures as needed throughout the duration of an incident. • Define and communicate clear roles and responsibilities relative to courses of action. • Prioritize and synchronize actions to ensure unity of effort. • Ensure clear lines and modes of communication between entities, both horizontally and vertically. • Ensure appropriate private sector participation in operational coordination throughout the cyber incident response cycle consistent with the NIPP. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Perform table-top activities to verify and validate effective and appropriate coordination between stakeholders.
10. Planning Description: Conduct a systematic process engaging the whole community, as appropriate, in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.
Critical Tasks: • Initiate a flexible planning process that builds on existing plans as part of the National Planning System.44 • Collaborate with partners to develop plans and processes to facilitate coordinated incident response activities. • Establish partnerships that coordinate information sharing between partners to restore critical infrastructure within single and across multiple jurisdictions and sectors. • Inform risk management response priorities with critical infrastructure interdependency analysis. • Identify and prioritize critical infrastructure and determine risk management priorities. • Conduct cyber vulnerability assessments, perform vulnerability and consequence analyses, identify capability gaps, and coordinate protective measures on an ongoing basis in conjunction with the private and nonprofit sectors and local, regional/metropolitan, state, tribal, territorial, insular area, and federal organizations and agencies. • Develop operational, business/service impact analysis, incident action, and incident support plans at the federal level and in the states and territories that adequately identify critical objectives based on the planning requirements; provide a complete and integrated picture of the escalation and de-escalation sequence and scope of the tasks to achieve the objectives; and are implementable within the time frame contemplated in the plan using available resources. • Formalize partnerships such as memorandums of understanding or pre-negotiated contracts with governmental and private sector cyber incident or emergency response teams to accept, triage, and collaboratively respond to incidents in an efficient manner. • Formalize partnerships between communities and disciplines responsible for cybersecurity and for physical systems dependent on cybersecurity. Formalize relationships such as memorandums of understanding or pre-negotiated contracts between information communications technology and information system vendors and their customers for ongoing product cyber security, business planning, and transition to response and recovery when necessary. • Formalize partnerships with government and private sector entities for data and threat intelligence sharing, prior to, during, and after an incident. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
11. Public Information and Warning Description: Deliver coordinated, prompt, reliable, and actionable information to the whole community and the public, as appropriate, through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding

significant threat or malicious cyber activity, as well as the actions being taken and the assistance being made available, as appropriate.
Critical Tasks: • Establish accessible mechanisms and provide the full spectrum of support necessary for appropriate and ongoing information sharing among all levels of government, the private sector, faith-based organizations, nongovernmental organizations, and the public. • Share actionable information and provide situational awareness with the public, private, and nonprofit sectors, and among all levels of government. • Leverage all appropriate communication means, such as the Integrated Public Alert and Warning System, public media, and social media sites. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Respect applicable information sharing and privacy protections, including Traffic Light Protocol. • Assure availability of redundant options to achieve critical public information, threat indication, and warning outcomes.
12. Screening, Search, and Detection Description: Identify, discover, or locate threats of malicious cyber activity through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, sensor technologies, or physical investigation and intelligence.
Critical Tasks: • Locate persons and networks associated with cyber threats. • Develop relationships and further engage with critical infrastructure participants (private industry and SLTT partners). • Conduct physical and electronic searches as authorized by law • Collect and analyze information provided. • Detect and analyze malicious cyber activity and support mitigation activities. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.
13. Situational Assessment Description: Provide all decision makers with decision-relevant information regarding the nature and extent of the malicious cyber activity, any cascading effects, and the status of the response.
Critical Tasks: • Coordinate the production and dissemination of modeling and effects analysis to inform immediate cyber incident response actions. • Maintain standard reporting templates, information management systems, essential elements of information, and critical information requirements. • Develop a common operational picture for relevant incident information shared by more than one organization. • Coordinate the structured collection and intake of information from multiple sources for inclusion into the assessment processes. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
14. Threats and Hazards Identification Description: Identify the threats of malicious cyber activity to networks and system; determine the frequency and magnitude; and incorporate this into analysis and planning processes so as to clearly understand the needs of an entity.
Critical Tasks: • Identify data requirements across stakeholders.

- Develop and/or gather required data in a timely and efficient manner to accurately identify cyber threats.
- Ensure that the right people receive the right data at the right time.
- Translate data into meaningful and actionable information through appropriate analysis and collection tools to aid in preparing the public.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Discover, evaluate, and resolve gaps in policy, facilitate or enable technologies, partnerships, and procedures which are barriers to effective threat, vulnerability, and hazard identification for the sectors.

GUIDANCE ON REPORTING A CYBER DISRUPTION

ESCALATION

A cyber disruption should be reported if it was determined that the affected entity has experienced the following impact upon detection:

Functional Impact	• Incidents impacting the business functionality of critical IT systems resulting in some type of negative impact to the users, business processes, etc. (e.g. DDoS, Ransomware, etc.)
Information Impact	• Incidents that affect the confidentiality, integrity, and availability of the entity's information resources (e.g. DDoS, Ransomware, etc.)
Recoverability Efforts	• It is not possible to recover from an incident due to unforeseen circumstance as it would require addition resources on the incident handling cycle; unless that effort was directed at ensuring that a similar incident did not occur in the future.

COMMUNICATION

The reporting entity should maintain records about the status of incidents, along with other pertinent information. The incident report should contain information on the following:

- Brief description of the incident and what was impacted
- Contact information for all parties involved
- Status of the incident (If possible, other incidents related to this incident)
- Indicators related to the incident (e.g. malicious IP addresses, domains, hashes etc.)
- Actions taken by all incident handlers on this incident (e.g. chain of custody and comments from incident handlers, etc.)
- A list of evidence gathered during the incident investigation (e.g. forensic acquisitions, network logs, etc.)

THREAT LEVELS AND ANTICIPATED RESPONSE

Threat Level	Description	Potential Impact	Communication Activity	Anticipated Response Activity
Emergency	Poses an imminent threat to the provision of wide-scale critical infrastructure services	Widespread outages, and/or destructive compromise to systems with no known remedy, or one or more critical infrastructure sectors debilitated	State EOC coordinates all communications CSTF activities	State EOC, Governor's Unified Command activated and is represented at State EOC
Severe	Likely to results in a significant impact to public health and/or safety	Core infrastructure targeted or compromised causing multiple outages, multiple system compromises or critical infrastructure compromises	- Notify and convene by phone or in person - DAGS/ETS to activate CSTF and report incident to MS-ISAC, HSFC & HI-EMA	- Voluntary resource collaboration among CSTF members - Info sharing - Communications/messaging - Possible State EOC Activation
High	Likely to result in a discernable impact to public health, safety or confidence	Compromised systems or diminished services	- Notify DAGS/ETS - ETS-CST to report incident to MS-ISAC - CSTF may be activated at this level	Real-time collaboration via phone and email as required. Activity can be conducted remotely.
Medium	May affect public health, safety, and/or confidence	Potential for malicious cyber activities, no known exploits, or known exploits, identified but no significant impact has occurred.	- Contact DAGS/ETS and share with affected department/agencies and any that may be affected. - ETS-CST to report incident to MS-ISAC	Informational only. No follow-up activity required. No real-time collaboration.
Low	Unlikely to affect public health, safety, and/or confidence	Normal concern for known hacking activities, known viruses, or other malicious activity	- Contact DAGS/ETS if discovered by another State dept/agency	None expected

Table 1 State of Hawai'i Cyber Security Response Matrix

The table above provides the Cyber Security Threat Levels identified for the State of Hawaii, with potential impacts and general anticipated response activity.

The State of Hawaii Cyber Security Response Matrix consists of 5 distinct levels, which are affected by internal and/or external cyber security events. The matrix provides general guidance of the communication and anticipated responses activities for each threat level. This section provides the following information for each threat level:

- Level definition – a brief description of what each security level means;
- Escalation/De-escalation criteria – description of the variables that are in place for alert level to change;
- Potential impact – how the level affects state agencies, municipalities, and the public;
- Communications procedures – how the knowledgeable party communicates with the ETS-CST, CSTF, the HSFC, or other response partners in order to inform affected individuals and organizations of the threat;

It is important to note that these threat levels are based on the risk an event poses and the impact it has, particularly on the state government enterprise. Incidents may require the ETS-CST and/or CSTF to skip levels, and/or to address an intervening threat before returning to the originating level after that threat has been mitigated.

1. CYBER SECURITY THREAT LEVEL – EMERGENCY

At Level EMERGENCY, unknown vulnerabilities are being exploited causing widespread damage and disrupting critical state government information technology infrastructure and assets. These attacks have an impact at the national, state, and local levels.

If a Cyber Security Threat Level EMERGENCY occurs within the state information technology enterprise _____ must be notified of the incident as soon as possible. _____ will be informed as part of the response process.

- Definition: Malicious activity has been identified with a catastrophic level of damage or Incident. Examples include but are not limited to:
  - Malicious activity results in widespread outages and/or complete network failures;
  - Data exposure with severe impact;

  - Significantly destructive compromises to systems, or disruptive activity with no known remedy;
  - Mission critical application failures with imminent or demonstrated impact on the health, safety, or economic security of the state;
  - Compromise or loss of administrative controls of critical system;
  - Loss of critical Land Mobile Radio and other critical State infrastructure.
- Actions:
  - Continue recommended actions from previous levels; Data exposure with severe impact;
  - Shut down connections to the Internet and external business partners until appropriate corrective actions are taken;
  - Ensure that potential threats are disseminated and outreach for prevention purposes is made to other entities;
  - Contact appropriate law enforcement partners to pursue enforcement actions through investigation and criminal prosecution;
  - Isolate internal networks to contain or limit the damage or Incident.
  - Governor to initiate Robert T. Stafford Relief and Emergency Assistance Act
- Escalation: To raise the threat level to Level EMERGENCY, the following conditions must be in place: The threat has affected multiple agencies and/or could require the state to shut down the IT infrastructure for six to thirty business days to restore normal business operations.
- Potential Impact:
  - Impact to IT Services:
    - Telecommunications are unavailable making it necessary to use alternate forms of communication;
    - The power grid is unreliable causing agencies to rely on backup generators or uninterrupted power supply (UPS);
    - Buildings have been damaged or destroyed rendering IT resources inoperable;
    - Relocation to State EOC for command and control purposes; Agency(ies) Incident/Incident Response Plan(s) activated;
    - Response activities must be implemented to restore IT operations and/or to address damages from the cyber-attack;
    - Data centers have to be restored or relocated to alternate facilities;
    - The issues raised by the Incident will take over six business days to remediate and critical applications and services will be offline until the issues are resolved;
    - The threat can only be remediated by restoring the applications systems, and facilities to an operational state by rebuilding equipment or restoring critical systems or applications to a previous date before the attacks occurred.
  - Agency Impact:
    - Agency IT staff will work to restore equipment, systems, and applications to an operational state;

  - Agencies will work with the Governor's Unified Command and Attorney General to address any ramifications, including political and legal issues, which may arise from the Incident.
- Communications Procedures: At Level EMERGENCY, he state/municipal critical IT resources are rendered inoperable by a cyber security attack that will take weeks to recover. Such an event will affect IT communications and necessitate the need for alternate forms of communication (e.g., satellite, radios, messengers).
  - State EOC – The State EOC will be activated, and the following State EOP, the Governor's Unified Command will meet there.
  - Work with the State EOC to establish temporary communications for recovery personnel, including issuing radios to responders assisting in the recovery process.
  - CIO will ensure that MS-ISAC is notified, and request assistance if necessary.
  - Pursuant to the State EOP, a WebEOC incident may be opened and WebEOC used to provide situational awareness, process requests for assistance, etc.
  - Telecommunications may become unreliable making it necessary for incident responders and first responders alike to use alternate forms of communication;
  - Messengers-Depending on the nature of the event, the state may use messengers to communicate information between incident responders and the State EOC.
- De-Escalation Criteria: To return to Level SEVERE or below, the Incident must pass the escalation criteria identified within each section.

2. CYBER SECURITY THREAT LEVEL – SEVERE

Level SEVERE signifies confirmed cyber-attacks are disrupting federal, state, and local government communications; and/or unknown exploits have compromised (state/municipal) IT resources and are using them to propagate the attack or to spread misinformation.

If a Cyber Security Threat Level SECURE occurs within the state information technology enterprise, _____ , and _____ must be notified of the incident as soon as possible. The Hawaii State Fusion Center shall be informed as part of the response process.

- Definition: Malicious activity has been identified in (state/municipal) networks with a major level of damage or Incident. Examples include but are not limited to:
  - Malicious activity affecting core infrastructure;
  - A vulnerability is being exploited and there has been major impact;
  - Data exposed with major impact;
  - Multiple system compromises or compromises of critical infrastructure;
  - Attackers have gained administrative privileges on compromised systems in multiple locations;

- Multiple damaging or disruptive malware infections;
- Mission critical application failures but no imminent impact on the health, safety, or economic security of the state;
- A distributed denial of service attack with major impact.

- Actions:
  - Refer to Matrix in Table 1 for communications flow;
  - Continue recommended actions from previous levels;
  - Agency(ies) Incident/Incident Response Plan(s) activated;
  - Closely monitor security mechanisms including firewalls, web log files, anti-virus gateways, and system log files for unusual activity;
  - Consider limiting or shutting down less critical connections to external networks such as the internet;
  - Consider isolating less mission critical internal networks to contain or limit the potential of an incident;
  - Fax, phone (where available) or state radio network in lieu of email and other forms of electronic communication;
  - When available, test and implement patches, anti-virus updates, and other measures immediately;
  - State EOC activation based on conditions, following the State EOP. Voluntary resource collaboration, technical information sharing and resource deployment, including mutual aid if needed. May include financial considerations.
  - Governor to consider initiating Robert T. Stafford Relief and Emergency Assistance Act if deemed necessary.
- Potential Impact:
  - Impact to IT Services could include:
    - A critical vulnerability is being exploited and there has been a significant impact;
    - Telecommunications may be interrupted causing agencies to use alternate forms of communication;
    - Email communications may be disrupted or untrusted, making it necessary for agencies affected by the event to use alternate forms of communications;
    - Relocation to the State EOC for command and control purposes;
    - Agency IT Operations may have to be relocated to the State EOC for command and control purposes;
    - Response activities may have to be implemented to restore IT operations and/or to address damages from the cyber-attack;
    - Normal grid supplied power may become unreliable/unavailable for extended periods of time and considerations of emergency backup power are being prioritized;
    - Multiple damaging or disruptive virus attacks; and/or multiple denial of service attacks against critical infrastructure services;

        - The threat can only be remediated by restoring the applications and systems to an operational state by rebuilding equipment, restoring critical systems or applications to a previous date before the attacks occurred;
    - Agency Impact:
        - Agency IT staff will work with ETS to restore equipment, systems, and applications to an operational state;
        - Agencies will work with the Governor's Unified Command and Attorney General to address any ramifications, including political and legal issues that may arise from the Incident.
    - Municipal Sector:
        - Impacts to municipal infrastructure and operations will be monitored following the State EOP, and requests for mutual aid will be received for consideration at the State EOC, including assistance to contain or address the cyber incident.
- Communication Procedures: At Level SEVERE, the (state/municipal) IT critical resources have been severely affected by a cyber security event that has caused IT service to be offline/unreliable for an extended period. This event may affect telecommunications and may cause incident responders to use alternate forms of communication.
    - The responding personnel will be notified via email if available, cell phone or messenger, will activate the Incident Response Plan, and will recommend a State EOC activation.
    - The responding personnel will work with the State EOC to establish temporary communications for recovery personnel, including issuing radios to responders assisting in the recovery process.
    - Senior responding personnel or CIO will ensure that MS-ISAC is notified, and request assistance if necessary.
    - Email will be used if available to communicate alerts, status reports, updates, and ancillary information.
    - Pursuant to the State EOP, a WebEOC incident may be opened and WebEOC used to provide situational awareness, process requests for assistance, etc.
    - Telecommunications may become unreliable making it necessary for incident responders and first responders alike to use alternate forms of communication;
    - Messengers – Depending on the nature of the event, the state may use messengers to communicate information among incident responders, the responding personnel, and the State EOC.
- De-Escalation Criteria: To return to Level HIGH or below, the incident must pass the escalation criteria identified within that section.

3. CYBER SECURITY THREAT LEVEL – HIGH

If a Cyber Security Threat Level HIGH occurs within the state information technology enterprise, _____ , _____ and, _____ shall be notified of the incident.

- Definition: Malicious activity has been identified in (state/municipal) networks with a moderate level of damage or Incident.
- Examples include but are not limited to:
  - An exploit for a vulnerability that has a moderate level of damage;
  - Compromise of secure or critical system(s);
  - Compromise of systems containing sensitive information or non-sensitive information;
  - More than one agency affected in the (state/municipal) network with moderate level of impact;
  - Infected by malware spreading quickly throughout the Internet with moderate impact;
  - A distributed denial of service attack with minor impact.
- Actions:
  - Refer to Matrix in Table 1 for communications flow;
  - Continue recommended actions from previous levels;
  - Agency(ies) Incident/Incident Response Plan(s) activated identify vulnerable systems;
  - Increase monitoring of critical systems;
  - Contact senior responding personnel for additional guidance;
  - Immediately implement appropriate counter-measures to protect vulnerable critical systems;
  - When available, test and implement patches, install anti-virus updates, and other system security measures as soon as possible;
  - Contact DAGS/ETS. HSFC and HI-EMA will be contacted for situational awareness and information sharing regarding potential threats and outreach to other entities for prevention purposes;
  - Real time collaboration via phone and email as required;
  - Consider State EOC activation;
  - Governor to consider initiating Robert T. Stafford Relief and Emergency Assistance Act if deemed necessary.
- Escalation Criteria: In order to raise the state/municipal agency threat level to Level HIGH, the threat must involve two or more agencies or critical infrastructure sectors, critical applications, or websites; and/or the risk of the threat has been determined to have a significant impact to (state/municipal) IT operations.
- Potential Impact: At Level HIGH, the following conditions are in place:
  - Impact to IT Services could include:

- There are multiple web defacements;
- A critical vulnerability is being exploited and there has been moderate impact;
- Attackers have gained administrative privileges on compromised systems;
- Critical applications or resources have been affected;
- Compromise of secure or critical system(s) containing sensitive information;
- Compromise of critical system(s) containing non-sensitive information, if appropriate;
- IT services may be interrupted by denial of service attacks;
- The issue can be remediated within one to three business days and may require that critical application or services be taken offline until the issue can be remediated;

  - Continuity of Operations Plan(s)/Continuity of Government Plans(s) (COOP)/COG) may have to be initiated to address the damages from the cyber-attack.
  - Remediation Effort: The threat can be remediated by (state/municipal) agencies installing software patches, updating anti-virus files, or denying network access to specific Ips or IP ranges.
  - Agency Impact:
    - Agency IT staff will work DAGS/ETS CSTF and with Subject Matter Experts (SMEs) from various agencies to install software patches, update anti-virus files, or deny network access to specific Ips or IP ranges;
    - Agency(ies) Incident/Incident Response Plan(s) activated;
    - If state is affected responding personnel will work with the Governor's Office /Unified Command and the Attorney General to address any ramifications, including political or legal issues that may arise from the incident;
  - Responding personnel will work with State EOC, if activated, to address any communication or facility needs required by the agency to address the Incident.

- Communication Procedures: At Level HIGH situation means that some of the (state/municipal) IT critical resources have been affected by a cyber security event or that multiple agencies have had significant security breaches. At this level, the following communications methods may be utilized:
  - Refer to Matrix in Table 1 for communications flow, which includes:
    - The CSTF will be convened by the State CIO via email, telephone, cell phone or messenger and the Team will start making preparations to enact the State Cyber Incident Response Plan and this CIRP.
    - Senior responding personnel or CIO will ensure that responding personnel are notified. Responding personnel may also request assistance with remediating the issue;
    - Responding personnel, through HSFC or other means, will notify designated individuals/groups and provide it with updates or remediation information;

  - Email will be used to communicate alerts, status reports, updates and ancillary information. In case none of previously listed methods are available, mobile devices and LMR will be used as a means of communicating;
  - Telecommunications such as landlines and cell phones will be used for clarification purposes and to address questions about remediations efforts. In case none of previously listed methods are available, LMR will be used as a means of communicating;
- De-Escalation Criteria: To return to Level MEDIUM or below, the incident must pass the criteria defined within that section.

4. CYBER SECURITY THREAT LEVEL – MEDIUM

If a Cyber Security Threat Level MEDIUM occurs within the state information technology enterprise and can be handled without serious effects within the enterprise and without any external effects. The affected entity should notify ETS-CST for intelligence collection purposes, including monitoring trends.

- Definition: This is the first active threat level in the cyber security response matrix. Level MEDIUM means that malicious activity has been identified on state, municipal networks with minor impact.
- Examples include but are not limited to:
  - Change in normal activity with minor impact IT operations;
  - A critical vulnerability, with the potential to cause significant damage if exploited, has been detected;
  - A vulnerability is being exploited and there has been minor impact;
  - Infection by malware with potential to spread quickly;
  - Compromise of non-critical system(s) that did not result in loss of sensitive data;
  - A distributed denial of service attack with minor impact.
- Actions:
  - State agencies need to contact ETS-CST, which will interface with MS-ISAC for information sharing and additional guidance;
  - Continue recommended action from previous level;
  - Agency(ies) Incident/Incident Response Plan(s) activated;
  - Identify vulnerable systems and implement appropriate countermeasures;
  - Identify malware on system and remediate accordingly;
  - Document data exposure with minor impact;
  - When available, test and implement patches, install anti-virus updates, and other security measures in next regular cycle;

  - Contact only other agencies/departments if there is a potential to be affected as well.
- Escalation Criteria:
  - In order to raise the state agency threat level to Level MEDIUM, the State CIO or equivalent at government level must determine that the following conditions are in place: The threat is limited to one agency, application, or website; and/or the risk of threat is low and it can be easily remediated without having a long-term impact to state, municipal, or the State of Hawaii residents and/or visitors.
- Potential Impact: At Level MEDIUM, the following conditions are in place:
  - Impact to IT services:
    - There is no threat to mission critical applications or resources;
    - The issue has been properly identified and can easily be remediated without risk of a data breach or theft of services;
    - The issue can be remediated within normal business hours;
    - The threat can be easily remediated by State agencies following normal procedures (e.g. software patches, updating virus files).
  - Special Events/Circumstances: A special event or circumstance incites hackers interested in trying to disrupt an agency IT services or deface a website, etc.
  - Agency impact: IT staff will take proactive measures. Impact to IT services should be minimal sine the threat has been identified and countermeasures exist for remediation.
- Communication Procedures: All IT resources are still operational. Communications will proceed as usual, with notification to ETS-CST, affected department/agencies, MS-ISAC and other partners as appropriate. See Table 1 Matrix. Email will be used to provide any alerts, status reports, updates and ancillary information to critical infrastructure owners and operators. Landlines and cell phone will be used for any clarification purposes and to address questions about remediation efforts.
- De-Escalation Criteria: To return to Level – LOW, any issues must be completely resolved, and agencies must confirm that IT resources are working normally and/or the circumstance has passed.

5. CYBER SECURITY THREAT LEVEL – LOW

Agencies and organizations conduct the following activities on an ongoing basis:

If a Cyber Security Threat Level LOW occurs within the state information technology enterprise, and can be handled without negative impacts outside the enterprise, no need to inform CSTF for intelligence collection purposes, including monitoring trends.

- Definition: Insignificant or no malicious activity has been identified. Examples include but are not limited to:
  - Credible warnings of increased probes or scans in a State, municipal network;
  - Infection by known low risk malware;
  - Other like incidents;
  - Normal activity with low level of impact.
- Actions:
  - Continue routine preventative measures;
  - Continue routine security monitoring;
  - Determine baseline of activity for the State/municipality/business—it is important to know what "normal" looks like;
  - State agencies need to contact ETS-CST, which will interface with MS-ISAC for information sharing and additional guidance if needed;
  - Ensure all personnel receive proper training on cyber security policies and security best practices.
- Escalation criteria: Infrastructure is operating normally and there are no known major cyber threats at this time
- De-Escalation criteria: In order to return to this level, the conditions that caused the change must be remediated.
- Potential impact: No cyber-related issues should be affecting state IT resources.
- Communication procedures: Besides day-to-day operational communications, no special communication procedures are required.

COMMUNICATIONS CHECKLISTS

A cyber disruption has the potential to cast a negative light on the State of Hawai'i - as well as to undermine faith in the State and possibly the Federal Government. If you are uncertain whether a situation could escalate into a crisis, err on the side of standing up response teams, because you can always stand down if the incident does not escalate. The checklists below can be adapted to account for various circumstances.

Action: Before a cyber crisis

- ☐ Identify protocol and the memberships of the technical response team(s).
- ☐ Create a list of terms with common cyber incident nomenclature for use by all stakeholders.
- ☐ Set an internal communication plan with key staff. (How often, when, and where will all staff meet? Information must travel up and down the chain of command with clear boundaries for dissemination and interfacing with the public/media.)
- ☐ Ensure that all stakeholders can be reached in a crisis without access to the affected systems, network or enterprise, including smart phones.
- ☐ Where appropriate and possible, establish contact with all appropriate entities responsible for cybersecurity. Also, understand in advance the legal obligations regarding the personal and/or sensitive data held by the organization.
- ☐ Establish contact with technology providers about potential threats and ensure that they know the technical and policy support functions available to them.
- ☐ Conduct briefings for members of the media.
- ☐ Get your social media account verified, because it will provide priority access to the helplines if your profile is compromised. Use social media to show how your organization is preparing.
- ☐ Raise awareness of tactics used in disinformation campaigns.
- ☐ Craft communications materials that can be used in a potential cyber disruption, including social media messages.
- ☐ Ensure that staff understand their role in a cyber disruption. For those who do not have a specific task to carry out, reassure them that their work is important and inform them how they can continue doing their jobs while designated managers handle the cyber disruption.
- ☐ Ensure that communications plans can be accessed and are regularly updated.

Action: Before a cyber crisis becomes public

- ☐ Obtain technical briefing. (Assess and verify all information.)
- ☐ Decide whether to activate technical response team(s).
- ☐ Decide whether website and social media accounts can remain online. If you must disable them, launch a microsite (hosted on a different network) in their place.
- ☐ If email is potentially compromised, use an outside communications channel such as a secure messaging app with end-to-end encryption.
- ☐ Consult appropriate government authorities.

- ☐ Meet internally in central meeting room; set internal communication schedule.
- ☐ Determine technical response team(s) roles and responsibilities, if you have not already done so.
- ☐ Determine and identify the appropriate stakeholders for the disruption response.
- ☐ Determine broad communications strategy.
- ☐ Prepare holding statement based on language you have already drafted.
- ☐ Develop communications plan.
- ☐ Draft additional communications required to execute plan, including a communications rollout plan (includes communication with media, stakeholders, and employees).
- ☐ Establish plan for traditional and social media monitoring.
- ☐ Establish media response protocol.
- ☐ Notify employees, if necessary. It may be that only a small group of employees are informed initially. Communicate internally, as needed.
- ☐ Notify stakeholders and galvanize support.
- ☐ Begin media (social and traditional) monitoring.

Action: Once a cyber disruption becomes public

- ☐ Fact check: Make sure communications materials reflect current facts.
- ☐ Execute rollout plan, including informing media, if appropriate.
- ☐ Determine if microsite/web page is needed.
- ☐ Record an office greeting for phone system, if necessary.
- ☐ Maintain a record of inbound media inquiries and responses, add bullets on feedback information from coverage, conversations with reporters and other data on external reaction.
- ☐ Continue media (social and traditional) monitoring.
- ☐ Review and revise messaging, as needed, based on feedback.

General Media Inquiries Checklist

Gather basic facts:

- ☐ Story topic/angle/deadline
- ☐ Platform (blog, newspaper, television, or radio) plus request content and images
- ☐ Other potential interview subjects
- ☐ Remember: Only designated spokespeople should speak or provide content.
- ☐ Remember: You have rights when you communicate with journalists, especially when asked about technical details you wouldn't be expected to know. "Let me see what I can find out for you" is always an option for a response. This may mean that you return to the reporter without any additional information. You are not obligated to provide details.
- ☐ Remember: Reporters are under pressure to produce a story and may shift the pressure to you. Do not speculate to fill gaps for them.

Notify key people:

- ☐ Meet internally.
- ☐ Craft media plan. Includes internal plans for staff and stakeholder communications.
- ☐ Designate key spokespeople and content providers. Assign tasks.
- ☐ Assist in crafting messaging. Reflect key audiences, people affected now, and those who will be affected in the future.
- ☐ Media
- ☐ Government offices
- ☐ Vendors
- ☐ General Public
- ☐ Demonstrate leadership by describing the steps you are taking to address this cyber incident. Consider contacting stakeholders who may be affected, especially if you think they may dislike or disagree with your messages.

The Department of Homeland Security
Notice of Funding Opportunity
Fiscal Year 2022 State and Local Cybersecurity Grant Program

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. Detailed information regarding UEI and SAM is also provided in Section D of this notice.

Table of Contents

A. Program Description

1. Issued By
U.S. Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA)/Resilience/Grant Program Directorate (GPD)

2. Assistance Listings Number
97.137

3. Assistance Listings Title
State and Local Cybersecurity Grant Program (SLCGP)

4. Funding Opportunity Title
Fiscal Year 2022 State and Local Cybersecurity Grant Program (SLCGP)

5. Funding Opportunity Number
DHS-22-137-000-01

6. Authorizing Authority for Program
Section 2220A of the Homeland Security Act of 2002, as amended (Pub. L. No. 107-296) (6 U.S.C. § 665g)

7. Appropriation Authority for Program
Infrastructure Investments and Jobs Appropriations Act (Pub. L. No. 117-58)

8. Announcement Type
Initial

9. Program Category
Preparedness: Community Security

10. Program Overview, Objectives, and Priorities

a. *Overview*

Our nation faces unprecedented cybersecurity risks, including increasingly sophisticated adversaries, widespread vulnerabilities in commonly used hardware and software, and broad dependencies on networked technologies for the day-to-day operation of critical infrastructure. Cyber risk management is further complicated by the ability of malicious actors to operate remotely, linkages between cyber and physical systems, and the difficulty of reducing vulnerabilities.

The potential consequences of cyber incidents threaten national security. Strengthening cybersecurity practices and resilience of state, local, and territorial (SLT) governments is an important homeland security mission and the primary focus of the State and Local Cybersecurity Grant Program (SLCGP). Through funding from Infrastructure Investment and Jobs Act (IIJA), also known as the Bipartisan Infrastructure Law (BIL), the SLCGP enables DHS to make targeted cybersecurity investments in SLT government agencies, thus improving the security of critical infrastructure and improving the resilience of the services

SLT governments provide their community.

The FY 2022 SLCGP aligns with the 2020-2024 DHS Strategic Plan by helping DHS achieve Goal 3: Secure Cyberspace and Critical Infrastructure, Objective 3.3. Assess and Counter Evolving Cybersecurity Risks. The FY 2022 SLCGP also supports the 2022-2026 FEMA Strategic Plan which outlines a bold vision and three ambitious goals, including Goal 3: Promote and Sustain a Ready FEMA and Prepared Nation, Objective 3.2: Posture FEMA to meet current and emergent threats.

b. ***Objectives***

The goal of SLCGP is to assist SLT governments with managing and reducing systemic cyber risk. For Fiscal Year (FY) 2022, applicants are required to address how the following program objectives 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.

For more information on the program goals, objectives, sub-objectives, and desired outcomes, please refer to Appendix A.

c. ***Priorities***

The Homeland Security Act of 2002, as amended by the Bipartisan Infrastructure Law requires grant recipients to develop a Cybersecurity Plan, establish a Cybersecurity Planning Committee to support development of the Plan, and identify projects to implement utilizing SLCGP funding. To support these efforts, recipients are highly encouraged to prioritize the following activities using FY 2022 SLCGP funds, all of which are statutorily required as a condition of receiving a grant:

- Establish a Cybersecurity Planning Committee;
- Develop a state-wide Cybersecurity Plan, unless the recipient already has a state-wide Cybersecurity Plan and uses the funds to implement or revise a state-wide Cybersecurity Plan;
- Conduct assessment and evaluations as the basis for individual projects throughout the life of the program; and
- Adopt key cybersecurity best practices.

Cybersecurity Planning Committee

The Planning Committee is responsible for developing, implementing, and revising Cybersecurity Plans (including individual projects); formally approving the Cybersecurity Plan (along with the chief information officer, chief information security officer or an

equivalent official); and assisting with determination of effective funding priorities (i.e., work with entities within the eligible entity's jurisdiction to identify and prioritize individual projects). To support these responsibilities, the Planning Committee must include the following entities:

- The eligible entity (i.e., state or territory);
- County, city, and town representation (if the eligible entity is a state);
- Institutions of public education within the eligible entity's jurisdiction;
- Institutions of public health within the eligible entity's jurisdiction; and
- As appropriate, representatives from rural, suburban, and high-population jurisdictions.

For more information on the Cybersecurity Planning Committee responsibilities and composition, please refer to Appendix B.

Cybersecurity Plan

To assist in developing the required Plan, a Cybersecurity Plan Checklist containing information on what must be included in the Plan has been developed for use by SLCGP recipients. Recipients are encouraged to incorporate, where applicable, any existing plans to protect against cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, SLT governments. For more information on the Cybersecurity Plan and Cybersecurity Plan Checklist, please refer to Appendix C.

Key Cybersecurity Best Practices

To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, SLT governments must take decisive steps to modernize their approach to cybersecurity, adopting security best practices and advancing toward Zero Trust Architecture. The following strategic elements, therefore, are required to be included in Cybersecurity Plans and in individual projects:

- Implement multi-factor authentication;
- Implement enhanced logging;
- Data encryption for data at rest and in transit;
- 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 (backups); and
- Migration to the .gov internet domain.

As individual government entities increase their cybersecurity maturity, implementing more advanced best practices, such as endpoint detection and response capabilities, as well as conducting regular penetration testing, will be recommended.

11. Performance Measures

Each grant recipient is required to collect data to allow DHS to measure performance of the awarded grant in support of the SLCGP metrics, which will be described in each Cybersecurity Plan.

The statute requires that "not later than one year after the date on which an eligible entity receives a grant…for the purpose of implementing [its] Cybersecurity Plan…, including an eligible entity that comprises a multi-entity group that receives a grant for that purpose, and annually thereafter until one year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report that, using the metrics described in the Cybersecurity Plan of the eligible entity, describes the progress of the eligible entity in:

- Implementing the Cybersecurity Plan;
- Reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a state, local governments within the jurisdiction of the eligible entity."

If an eligible entity does not have a Cybersecurity Plan in place and receives an award, then the statute requires that not later than one year after the date on which the eligible entity receives a grant, and annually thereafter until one year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report describing how the eligible entity obligated and expended grant funds to:

- Develop or revise a Cybersecurity Plan; or
- Assist with activities that address imminent cybersecurity threats, as confirmed by the Secretary, acting through the CISA Director, to the information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity.

In order to measure performance, DHS may request information throughout the period of performance. In its final performance report submitted at closeout, the recipient must submit sufficient information to demonstrate it has met the performance goals as stated in its award. DHS will measure the recipient's performance of the grant by comparing the number of activities and projects needed and requested in its investment justification with the number of activities and projects acquired and delivered by the end of the period of performance using the following programmatic metrics:

- Percentage of entities with CISA approved state-wide Cybersecurity Plans
- Percentage of entities with statewide cybersecurity planning committees that meet the Homeland Security Act of 2002 and this SLCGP Notice of Funding Opportunity (NOFO) requirements
- Percentage of entities conducting annual table-top and full-scope exercises to test cybersecurity plans; Percent of the entities' SLCGP budget allocated to exercises; or Average dollar amount expended on exercise planning for entities

- Percentage of entities conducting an annual cyber risk assessment to identify cyber risk management gaps and areas for improvement
- Percentage of entities performing phishing training; Percent of entities conducting awareness campaigns; Percent of entities providing role-based cybersecurity awareness training to employees
- Percentage of entities adopting the Workforce Framework for Cybersecurity (NICE Framework) as evidenced by established workforce development and training plans
- Percentage of entities with capabilities to analyze network traffic and activities related to potential threats
- Percentage of entities implementing multi-factor authentication (MFA) for all remote access and privileged accounts
- Percentage of entities with programs to anticipate and discontinue use of end of life software and hardware
- Percentage of entities prohibiting the use of known/fixed/default passwords and credentials
- Percentage of entities operating under the ".gov" internet domain
- Number of cybersecurity gaps or issues addressed annually by entities

B. Federal Award Information

1. Available Funding for the NOFO: **$185 million**

For FY 2022, DHS will award state and territorial funds based on baseline minimums and population as required by the Homeland Security Act of 2002, and described below.

Each state and territory will receive a baseline allocation using thresholds established in the Homeland Security Act of 2002. All 50 States, the District of Columbia, and the Commonwealth of Puerto Rico will receive a minimum of $2,000,000 each, equaling 1% of total funds appropriated to DHS in FY 2022. Each of the four territories (American Samoa, Guam, the Northern Mariana Islands, and the U.S. Virgin Islands) will receive a minimum of $500,000, equaling 0.25% of the total funds appropriated to DHS in FY 2022. $90,500,000, 50% of the remaining amount will be apportioned based on the ratio that the population of each state or territory bears to the population of all states and territories. The remaining $90,500,000, equaling the other 50% of the remaining amount, will be apportioned based on the ratio that the population of each state that resides in rural areas bears to the population of all states that resides in rural areas.

FY 2022 SLCGP Allocations

State/Territory	FY 2022 SLCGP Allocation
Alabama	$3,848,596
Alaska	$2,245,130
Arizona	$3,336,349
Arkansas	$3,162,746
California	$7,981,997

State/Territory	FY 2022 SLCGP Allocation
Colorado	$3,234,143
Connecticut	$2,681,116
Delaware	$2,224,803
District of Columbia	$2,081,394
Florida	$5,889,464
Georgia	$4,877,389
Hawaii	$2,243,739
Idaho	$2,550,109
Illinois	$4,404,622
Indiana	$3,949,173
Iowa	$3,073,518
Kansas	$2,820,015
Kentucky	$3,659,521
Louisiana	$3,327,540
Maine	$2,666,932
Maryland	$3,214,008
Massachusetts	$3,173,589
Michigan	$4,777,219
Minnesota	$3,606,482
Mississippi	$3,274,355
Missouri	$3,841,132
Montana	$2,428,110
Nebraska	$2,555,930
Nevada	$2,488,375
New Hampshire	$2,499,170
New Jersey	$3,380,963
New Mexico	$2,540,767
New York	$5,813,554
North Carolina	$5,362,452
North Dakota	$2,287,118
Ohio	$4,980,243
Oklahoma	$3,294,613
Oregon	$2,988,975
Pennsylvania	$5,207,249
Rhode Island	$2,190,484
South Carolina	$3,661,568
South Dakota	$2,341,978
Tennessee	$4,244,182
Texas	$8,469,945
Utah	$2,619,397
Vermont	$2,310,302
Virginia	$4,292,938
Washington	$3,667,735

State/Territory	FY 2022 SLCGP Allocation
West Virginia	$2,764,988
Wisconsin	$3,795,634
Wyoming	$2,200,558
Puerto Rico	$2,492,381
U.S. Virgin Islands	$500,000
American Samoa	$500,000
Guam	$500,000
Northern Mariana Islands	$500,000
Total	**$185,024,690**

2. Projected Number of Awards: **56**

3. Period of Performance: **48 months**
Extensions to the period of performance are allowed. For additional information on period of performance extensions, please refer to Section H of this NOFO.

FEMA awards under most programs, including this program, only include one budget period, so it will be same as the period of performance. *See* 2 C.F.R. § 200.1 for definitions of "budget period" and "period of performance."

4. Projected Period of Performance Start Date(s): **Sept. 1, 2022**

5. Projected Period of Performance End Date(s): **Aug. 31, 2026**

6. Funding Instrument Type: **Grant**

C. Eligibility Information

1. Eligible Applicants

All 56 states and territories, including any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands, are eligible to apply for SLCGP funds. Accordingly, the Governor designated State Administrative Agency (SAA) is the only entity eligible to submit SLCGP applications to DHS/FEMA.

Although Tribes are not eligible to apply directly for SLCGP funding, they may be eligible subrecipients, and can receive SLCGP funding as a local government. Each individual SAA may determine whether and how much SLCGP funding to pass through to Tribal entities; DHS does not have the authority to mandate that a certain percentage of SLCGP funds are directed to Tribal governments. Additionally, $6 million in funding will be directly available to Tribal entities under the forthcoming Tribal Cybersecurity Grant Program, which DHS expects to publish the NOFO in the fall of 2022.

"State" is defined in 6 U.S.C. § 101(17) to include the 50 states, District of Columbia, Commonwealth of Puerto Rico, U.S. Virgin Islands, Guam, American Samoa, and Commonwealth of the Northern Mariana Islands;

"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 government" for purposes of being an eligible entity for the Tribal Cybersecurity Grant Program is defined in 6 U.S.C. § 665g(1)(12) as the recognized governing body of any Indian or Alaska Native Tribe, band, nation, pueblo, village, community, component band, or component reservation, that is individually identified (including parenthetically) in the most recent published list of Federally Recognized Tribes.

In addition to applying as a single entity, an eligible entity under SLCGP (i.e., the SAA) may partner with one or more other eligible entities to form a multi-entity group. Members of multi-entity groups work together to address cybersecurity risks and cybersecurity threats to information systems within their jurisdictions. There is no limit to the number of participating entities in a multi-entity group. Local entities can be included in the project, but their respective eligible entity must also participate at some level (see Appendix D). There is no separate funding for multi-entity awards. Instead, they should be considered as group projects within their existing state or territory allocations. These projects should be included as individual Investment Justifications from each participating eligible entity, each approved by the respective Planning Committee and aligned with each respective eligible entity's Cybersecurity Plan.

2. Applicant Eligibility Criteria

Applicants must be an eligible entity, meaning one of the 56 states and territories that are eligible for the program. One or more eligible entities may form a multi-entity group.

3. Other Eligibility Criteria

Cybersecurity Plan

To be eligible for FY 2022 SLCGP funding, each eligible entity is required to submit a Cybersecurity Plan that aligns with the criteria detailed in Appendix C.

The only exception is if an eligible entity certifies to the Secretary that:

A. The activities that will be supported by a grant are:
   1. Integral to the development of the Cybersecurity Plan of the eligible entity; or
   2. Necessary to assist with activities that address imminent cybersecurity threats, as confirmed by the Secretary, acting through the CISA Director, to the information systems owned or operated by, or on behalf of, the eligible entity or

a local government within the jurisdiction of the eligible entity; and

B. The eligible entity will submit to the Secretary a Cybersecurity Plan for review by September 30, 2023.

Note that for multi-entity groups, in order to be eligible for an award, all eligible entities within the multi-entity group must already have a Cybersecurity Plan in place; multi-entity groups are not eligible for awards to develop a Cybersecurity Plan. *See* 6 U.S.C. § 665g(f), (i)(3).

Cybersecurity Planning Committee

To be eligible for FY 2022 SLCGP funding, each eligible entity is required to establish a Cybersecurity Planning Committee comprised of the members summarized in Appendix B.

4. Cost Share or Match

Eligible entities, if applying as a single applicant, must meet a 10% cost share requirement for the FY 2022 SLCGP. The recipient contribution can be cash (hard match) or third-party in-kind (soft match). Eligible applicants shall agree to make available non-federal funds to carry out an SLCGP award in an amount not less than 10% of activities under the award. For FY 2022, in accordance with 48 U.S.C. § 1469a, cost share requirements **are waived for the insular areas** of the U.S. territories of American Samoa, Guam, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands.

DHS/FEMA administers cost-matching requirements in accordance with 2 C.F.R. § 200.306. To meet matching requirements, the recipient contributions must be verifiable, reasonable, allocable and necessary, and otherwise allowable under the grant program, and in compliance with all applicable federal requirements and regulations. Unless otherwise authorized by law, the non-federal cost share requirement cannot be matched with other federal funds.

For example, if the federal award were at a 90% cost share and the total approved budget cost was $100,000, then:

- Federal share is 90% of $100,000 = $90,000
- Recipient share is 10% of $100,000 = $10,000

However, with this example, if the total cost ended up being $120,000, the federal share would remain at $90,000 due to the statutory formula even if it means the federal share ends up being lower than 90%. Any cost overruns will not be matched by this grant program and will be incurred by the recipient. With this example, if the total cost ended up being $80,000, then the 90% federal share would decrease to $72,000, and the recipient cost share would be $8,000.

Additionally, by statute, the cost share applies to each individual activity funded by the grant award rather than just to the cumulative total. Recipients must ensure that each activity's cost share is met. DHS interprets "activity" to mean all items approved as part of a submitted "Project Worksheet."

For a multi-entity group project, a cost share or cost match is not required for the FY 2022 SLCGP. For more information about multi-entity group projects, please refer to Appendix D.

The Secretary of Homeland Security may waive or modify the non-federal share for an individual entity if the entity demonstrates economic hardship. Additional information about the eligibility criteria for a cost share waiver, as well as how to submit a request for a cost share waiver from DHS is included in Appendix H.

D. Application and Submission Information

1. Key Dates and Times

a. ***Application Start Date:*** 09/16/2022

b. ***Application Submission Deadline:*** ***11/15/2022 at 5 p.m. ET***

All applications **must** be received by the established deadline.

The Non-Disaster (ND) Grants System has a date stamp that indicates when an application is submitted. Applicants will receive an electronic message confirming receipt of their submission. For additional information on how an applicant will be notified of application receipt, see the subsection titled "Timely Receipt Requirements and Proof of Timely Submission" in Section D of this NOFO.

DHS will not review applications that are received after the deadline or consider these late applications for funding. DHS may, however, extend the application deadline on request for any applicant who can demonstrate that good cause exists to justify extending the deadline. Good cause for an extension may include technical problems outside of the applicant's control that prevent submission of the application by the deadline, other exigent or emergency circumstances, or statutory requirements for DHS to make an award.

Applicants experiencing technical problems outside of their control must notify DHS as soon as possible and before the application deadline. Failure to timely notify DHS of the issue that prevented the timely filing of the application may preclude consideration of the award. "Timely notification" of DHS means prior to the application deadline and within 48 hours after the applicant became aware of the issue.

A list of FEMA contacts can be found in Section G of this NOFO, "DHS Awarding Agency Contact Information." For additional assistance using the ND Grants System, please contact the ND Grants Service Desk at (800) 865-4076 or NDGrants@fema.dhs.gov. The ND Grants Service Desk is available Monday through Friday, 9 a.m. – 6 p.m. ET. If applicants have programmatic or grants management questions or concerns, please contact the Centralized Scheduling and Information Desk (CSID) by phone at (800) 368-6498 or by e-mail at askcsid@fema.dhs.gov, Monday through Friday, 9 a.m. – 5 p.m. ET.

c. ***Anticipated Funding Selection Date:*** No later than 11/30/2022

d. ***Anticipated Award Date:*** No later than 12/31/2022

e. ***Other Key Dates:***

Event	Suggested Deadline for Completion
Obtaining Unique Entity Identifier (UEI) Number	Four weeks before actual submission deadline
Obtaining a valid Employer Identification Number (EIN)	Four weeks before actual submission deadline
Creating an account with login.gov	Four weeks before actual submission deadline
Registering in SAM or updating SAM registration	Four weeks before actual submission deadline
Registering in Grants.gov	Four weeks before actual submission deadline
Registering in ND Grants	Four weeks before actual submission deadline
Starting application in Grants.gov	One week before actual submission deadline
Submitting the final application in ND Grants	By the submission deadline

2. Agreeing to Terms and Conditions of the Award

By submitting an application, applicants agree to comply with the requirements of this NOFO and the terms and conditions of the award, should they receive an award.

3. Address to Request Application Package

Initial applications are processed through the Grants.gov portal. Final applications are completed and submitted through FEMA's Non-Disaster Grants (ND Grants) System. Application forms and instructions are available at Grants.gov. To access these materials, go to http://www.grants.gov, select "Applicants" then "Apply for Grants". In order to obtain the application package, select "Download a Grant Application Package". Enter the Assistance Listing (formerly CFDA) and/or the funding opportunity number located on the cover of the program's NOFO, select "Download Package," and then follow the prompts to download the application package. In addition, the following Telephone Device for the Deaf (TDD) and/or Federal Information Relay Service (FIRS) number available for this Notice and all relevant NOFO is (800) 462-7585.

4. Steps Required to Obtain a Unique Entity Identifier, Register in the System for Award Management (SAM), and Submit an Application

Applying for an award under this program is a multi-step process and requires time to complete. Applicants are encouraged to register early as the registration process can take four weeks or more to complete. Therefore, registration should be done in sufficient time to ensure it does not impact your ability to meet required submission deadlines.

Please review the table above for estimated deadlines to complete each of the steps listed. Failure of an applicant to comply with any of the required steps before the deadline for submitting an application may disqualify that application from funding.
To apply for an award under this program, all applicants must:

a. Apply for, update, or verify their Unique Entity Identifier (UEI) number from SAM.gov and Employer Identification Number (EIN) from the Internal Revenue Service;
b. In the application, provide an UEI number;
c. Have an account with login.gov;
d. Register for, update, or verify their SAM account and ensure the account is active before submitting the application;
e. Create a Grants.gov account;
f. Add a profile to a Grants.gov account;
g. Establish an Authorized Organizational Representative (AOR) in Grants.gov;
h. Register in ND Grants
i. Submit an initial application in Grants.gov;
j. Submit the final application in ND Grants, including electronically signing applicable forms; and
k. Continue to maintain an active SAM registration with current information at all times during which it has an active federal award or an application or plan under consideration by a federal awarding agency. As part of this, applicants must also provide information on an applicant's immediate and highest-level owner and subsidiaries, as well as on all predecessors that have been awarded federal contracts or federal financial assistance within the last three years, if applicable.

Specific instructions on how to apply for, update, or verify a UEI number or SAM registration or establish an AOR are included below in the steps for applying through Grants.gov.

Applicants are advised that DHS may not make a federal award until the applicant has complied with all applicable SAM requirements. Therefore, an applicant's SAM registration must be active not only at the time of application, but also during the application review period and when DHS is ready to make a federal award. Further, as noted above, an applicant's or recipient's SAM registration must remain active for the duration of an active federal award. If an applicant's SAM registration is expired at the time of application, expires during application review, or expires any other time before award, DHS may determine that the applicant is not qualified to receive a federal award and use that determination as a basis for making a federal award to another applicant.

Per 2 C.F.R. § 25.110(c)(2)(iii), if an applicant is experiencing exigent circumstances that prevents it from receiving a UEI number, if applicable, and completing SAM registration prior to receiving a federal award, the applicant must notify FEMA as soon as possible by contacting askcsid@fema.dhs.gov and providing the details of the circumstances that prevent completion of these requirements. If FEMA determines that there are exigent circumstances and FEMA has decided to make an award, the applicant will be required to obtain a UEI number, if applicable, and complete SAM registration within 30 days of the federal award date.

5. Electronic Delivery

DHS is participating in the Grants.gov initiative to provide the grant community with a single site to find and apply for grant funding opportunities. DHS encourages or requires applicants

to submit their applications online through Grants.gov, depending on the funding opportunity.

For this funding opportunity, FEMA requires applicants to submit initial applications through Grants.gov and a final application through ND Grants.

6. How to Register to Apply through Grants.gov

a. ***General Instructions:***

Registering and applying for an award under this program is a multi-step process and requires time to complete. Read the instructions below about registering to apply for FEMA funds. Applicants should read the registration instructions carefully and prepare the information requested before beginning the registration process. Reviewing and assembling the required information before beginning the registration process will alleviate last-minute searches for required information.

The registration process can take up to four weeks to complete. To ensure an application meets the deadline, applicants are advised to start the required steps well in advance of their submission.

Organizations must have an UEI number, an EIN, an active SAM registration and Grants.gov account to apply for grants.

Organizations must also have a Grants.gov account to apply for an award under this program. Creating a Grants.gov account can be completed online in minutes, but DUNS and SAM registrations may take several weeks. Therefore, an organization's registration should be done in sufficient time to ensure it does not impact the entity's ability to meet required application submission deadlines. Complete organization instructions can be found on Grants.gov here: https://www.grants.gov/web/grants/applicants/organization-registration.html.

If individual applicants are eligible to apply for this grant funding opportunity, refer to:

b. ***Obtain an UEI Number:***

All entities applying for funding, including renewal funding, prior to April 4, 2022, must have a UEI number. Applicants must enter the UEI number in the applicable data entry field on the SF-424 form.

For more detailed instructions for obtaining a UEI number, refer to: Sam.gov.

c. ***Obtain Employer Identification Number***

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.

d. ***Create a login.gov account:***

Applicants must have a login.gov account in order to register with SAM or update their SAM registration. Applicants can create a login.gov account here:

https://secure.login.gov/sign_up/enter_email?request_id=34f19fa8-14a2-438c-8323-a62b99571fd3.

Applicants only have to create a login.gov account once. For applicants that are existing SAM users, use the same email address for the login.gov account as with SAM.gov so that the two accounts can be linked.

For more information on the login.gov requirements for SAM registration, refer to: https://www.sam.gov/SAM/pages/public/loginFAQ.jsf.

e. ***Register with SAM:***
All organizations applying online through Grants.gov must register with SAM. Failure to register with SAM will prevent your organization from applying through Grants.gov. SAM registration must be renewed annually.

For more detailed instructions for registering with SAM, refer to: https://www.grants.gov/web/grants/applicants/organization-registration/step-2-register-with-sam.html.

Note: As a new requirement per 2 C.F.R. § 25.200, applicants must also provide the applicant's immediate and highest-level owner, subsidiaries, and predecessors that have been awarded federal contracts or federal financial assistance within the last three years, if applicable.

I. Additional SAM Reminders

Existing SAM.gov account holders should check their account to make sure it is "ACTIVE." SAM registration should be completed at the very beginning of the application period and should be renewed annually to avoid being "INACTIVE." **Please allow plenty of time before the grant application submission deadline to obtain an UEI number, if applicable, and then to register in SAM. It may be four weeks or more after an applicant submits the SAM registration before the registration is active in SAM, and then it may be an additional 24 hours before FEMA's system recognizes the information.**

It is imperative that the information applicants provide is correct and current. Please ensure that your organization's name, address, and EIN are up to date in SAM and the UEI number used in SAM is the same one used to apply for all other FEMA awards. Payment under any FEMA award is contingent on the recipient's having a current SAM registration.

II. Help with 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.do or call toll free (866) 606-8220.

f. ***Create a Grants.gov Account:***
The next step in the registration process is to create an account with Grants.gov. If applicable, applicants must know their organization's DUNS number to complete this process.

For more information, follow the on-screen instructions or refer to:
https://www.grants.gov/web/grants/applicants/registration.html.

See also Section D.8 in this NOFO, "Submitting the Final Application in ND Grants," for instructions on how to register early in ND Grants.

g. ***Add a Profile to a Grants.gov Account:***
A profile in Grants.gov corresponds to a single applicant organization the user represents (i.e., an applicant) or an individual applicant. If you work for or consult with multiple organizations and have a profile for each, you may log in to one Grants.gov account to access all of your grant applications. To add an organizational profile to your Grants.gov account, if applicable, enter the DUNS number for the organization in the UEI field while adding a profile.

For more detailed instructions about creating a profile on Grants.gov, refer to:
https://www.grants.gov/web/grants/applicants/registration/add-profile.html.

h. EBiz POC Authorized Profile Roles:
After you register with Grants.gov and create an Organization Applicant Profile, the organization applicant's request for Grants.gov roles and access are sent to the EBiz POC. The EBiz POC will then log in to Grants.gov and authorize the appropriate roles, which may include the Authorized Organization Representative (AOR) role, thereby giving you permission to complete and submit applications on behalf of the organization. You will be able to submit your application online any time after you have been assigned the AOR role.

For more detailed instructions about creating a profile on Grants.gov, refer to:
https://www.grants.gov/web/grants/applicants/registration/authorize-roles.html.

i. ***Track Role Status:***
To track your role request, refer to:
https://www.grants.gov/web/grants/applicants/registration/track-role-status.html.

j. ***Electronic Signature:***
When applications are submitted through Grants.gov, the name of the organization applicant with the AOR role that submitted the application is inserted into the signature line of the application, serving as the electronic signature. The EBiz POC **must** authorize individuals who are able to make legally binding commitments on behalf of the organization as an AOR; **this step is often missed, and it is crucial for valid and timely submissions.**

7. How to Submit an Initial Application to DHS via Grants.gov
Standard Form 424 (SF-424) is the initial application for this NOFO.

Grants.gov applicants can apply online using a workspace. A workspace is a shared, online environment where members of a grant team may simultaneously access and edit different web forms within an application. For each Notice of Funding Opportunity, you can create individual instances of a workspace. Applicants are encouraged to submit their initial applications in Grants.gov ***at least*** seven days before the application deadline.

In Grants.gov, applicants need to submit the following forms:

- SF-424, Application for Federal Assistance; and
- Grants.gov Lobbying Form, Certification Regarding Lobbying.

Below is an overview of applying on Grants.gov. For access to complete instructions on how to apply for opportunities using Workspace, refer to: https://www.grants.gov/web/grants/applicants/workspace-overview.html

a. ***Create a Workspace:***
Creating a workspace allows you to complete it online and route it through your organization for review before submitting.

b. ***Complete a Workspace:***
Add participants to the workspace to work on the application together, complete all the required forms online or by downloading PDF versions, and check for errors before submission.

c. ***Adobe Reader:***
If you decide not to apply by filling out webforms you can download individual PDF forms in Workspace so that they will appear similar to other Standard or DHS forms. The individual PDF forms can be downloaded and saved to your local device storage, network drive(s), or external drives, then accessed through Adobe Reader.

NOTE: Visit the Adobe Software Compatibility page on Grants.gov to download the appropriate version of the software at: https://www.grants.gov/web/grants/applicants/adobe-software-compatibility.html

d. ***Mandatory Fields in Forms:***
In the forms, you will note fields marked with an asterisk and a different background color. These fields are mandatory fields that must be completed to successfully submit your application.

e. ***Complete SF-424 Fields First:***
The forms are designed to fill in common required fields across other forms, such as the applicant name, address, and UEI number. To trigger this feature, an applicant must complete the SF-424 information first. Once it is completed, the information will transfer to the other forms.

f. ***Submit a Workspace:***
An application may be submitted through workspace by clicking the "Sign and Submit" button on the Manage Workspace page, under the Forms tab. Grants.gov recommends submitting your application package at least 24-48 hours prior to the close date to provide you with time to correct any potential technical issues that may disrupt the application submission.

g. ***Track a Workspace:***
After successfully submitting a workspace package, a Grants.gov Tracking Number (GRANTXXXXXXXX) is automatically assigned to the application. The number will be listed on the confirmation page that is generated after submission. Using the tracking number, access the Track My Application page under the Applicants tab or the Details tab in the submitted workspace.

h. ***Additional Training and Applicant Support:***
For additional training resources, including video tutorials, refer to: https://www.grants.gov/web/grants/applicants/applicant-training.html
Grants.gov provides applicants 24/7 (except federal holidays) support via the toll-free number (800) 518-4726, email at support@grants.gov and the website at https://www.grants.gov/support.html. For questions related to the specific grant opportunity, contact the number listed in the application package of the grant you are applying for.

If you are experiencing difficulties with your submission, it is best to call the Grants.gov Support Center and get a ticket number. The Support Center ticket number will assist FEMA with tracking your issue and understanding background information on the issue.

8. Submitting the Final Application in ND Grants
After submitting the initial application in Grants.gov, eligible applicants will be notified by FEMA and asked to proceed with submitting their complete application package in ND Grants. Applicants can register early with ND Grants and are encouraged to begin their ND Grants registration at the time of this announcement or, at the latest, seven days before the application deadline. Early registration will allow applicants to have adequate time to start and complete their applications.

Applicants needing assistance registering for the ND Grants system should contact ndgrants@fema.dhs.gov or (800) 865-4076. For step-by-step directions on using the ND Grants system and other guides, please see https://www.fema.gov/grants/guidance-tools/non-disaster-grants-management-system.

In ND Grants, applicants will be prompted to submit the standard application information and any program-specific information required as described in Section D.10 of this NOFO, "Content and Form of Application Submission." The Standard Forms (SF) are auto generated in ND Grants, but applicants may access these forms in advance through the Forms tab under the SF-424 family on Grants.gov. Applicants should review these forms before applying to ensure they have all the information required.

For additional application submission requirements, including program-specific requirements, please refer to the subsection titled "Content and Form of Application Submission" under Section D of this NOFO.

9. Timely Receipt Requirements and Proof of Timely Submission

As application submission is a two-step process, the applicant with the AOR role who submitted the application in Grants.gov will receive an acknowledgement of receipt and a tracking number (GRANTXXXXXXXX) from Grants.gov with the successful transmission of its initial application. **This notification does not serve as proof of timely submission, as the application is not complete until it is submitted in ND Grants.** Applicants can also view the ND Grants Agency Tracking Number by accessing the Details tab in the submitted workspace section in Grants.gov, under the Agency Tracking Number column. Should the Agency Tracking Number not appear, the application has not yet migrated from Grants.gov into the ND Grants System. Please allow 24 hours for your ND Grants application tracking number to migrate.

All applications must be received in ND Grants by **5 p.m. ET** on the application deadline. Proof of timely submission is automatically recorded by ND Grants. An electronic date/time stamp is generated within the system when the application is successfully received by ND Grants. Additionally, the applicant(s) listed as contacts on the application will receive a system-generated email to confirm receipt.

10. Content and Form of Application Submission

a. ***Standard Required Application Forms and Information***

The following forms or information are required to be submitted in either Grants.gov or ND Grants. The Standard Forms (SF) are submitted either through Grants.gov, through forms generated in ND Grants, or as an attachment in ND Grants. Applicants may also access the SFs at https://www.grants.gov/web/grants/forms/sf-424-family.html.

I. GRANTS.GOV

- **SF-424, Application for Federal Assistance**, initial application submitted through Grants.gov; and
- **Grants.gov Lobbying Form, Certification Regarding Lobbying**, submitted through Grants.gov.

II. ND GRANTS

- **SF-424A, Budget Information (Non-Construction)**, submitted via the forms generated by ND Grants;
- **SF-424B, Standard Assurances (Non-Construction)**, submitted via the forms generated by ND Grants;
- **SF-LLL, Disclosure of Lobbying Activities**, submitted via the forms generated by ND Grants; and
- **Indirect Cost Agreement or Proposal**, submitted as an attachment in ND Grants if the budget includes indirect costs and the applicant is required to have an indirect cost rate agreement or proposal. If the applicant does not have or is not required to have an indirect cost rate agreement or proposal, please see Section D.13 of this NOFO, "Funding

Restrictions and Allowable Costs," for further information regarding allowability of indirect costs and whether alternatives to an indirect cost rate agreement or proposal might be available or contact the relevant FEMA staff identified in Section G of this NOFO, "DHS Awarding Agency Contact Information" for further instructions.

b. ***Program-Specific Required Forms and Information***

The following program-specific forms or information are required to be submitted in ND Grants as attachments:

- **SLCGP Investment Justifications**: Each eligible entity is required to submit complete project-level information detailing how the program objectives and goals will be met to develop, implement, or revise its Cybersecurity Plan; establish a Cybersecurity Planning Committee; conduct assessments and evaluations; and adopt key cybersecurity best practices. For more information on the Investment Justification, please refer to Appendix F. The FY 2022 Investment Justification must include the following information:
  - Only one application will be submitted by the eligible entity. It must include a brief description of the capabilities of the SLT agencies across the eligible entity related to the required elements of the Cybersecurity Plan.
  - The application will consist of up to four investments, one for each SLCGP objective (See Appendix F for more information on the goal and objectives).
  - Investments for SLCGP Objectives 1, 2, and 3 must have at least one project. Investments for SLCGP Objective 4 are optional for the FY 2022 SLCGP; however, it is important to note that identifying and mitigating gaps in the cybersecurity workforce, enhancing recruitment and retention efforts, and bolstering the knowledge, skills, and abilities of personnel are still statutory requirements for Cybersecurity Plans to address even if the eligible entity does not use grant funds to carry this out.
  - Requests to use funding to address imminent cybersecurity threats must be addressed in the Investment Justification (IJ) for Objective 3.
  - Each investment must describe how each project aligns to the entity's Cybersecurity Plan if applying for a grant to implement or revise the Cybersecurity Plan, or will align with the entity's Cybersecurity Plan if applying for a grant to develop a Cybersecurity Plan. Applicants must also describe how implementing the plan will be measured (metrics).
  - Each project must include an explanation of how the proposed project(s) will achieve the program objectives as identified in Appendix C. A project schedule with clearly defined milestones must also be included.
- **Cybersecurity Plan**: Each eligible entity is required to submit its Cybersecurity Plan that adheres to the 16 required elements identified in section 2220A of the Homeland Security Act of 2002 as amended by the BIL and included in Appendix C of this NOFO unless the eligible entity is applying for funds to develop a Cybersecurity Plan as described more below. The Cybersecurity Plan must include a description of SLT roles, an assessment of capabilities for each element, address resources and timeline for implementing the Plan, and identify metrics. SLT governments are encouraged to take a holistic approach in the development of their Plan as entities must be able to sustain capabilities once SLCGP funds are no longer available. The role of state entities as coordinator and service provider to local entities should be encouraged and supported.

For more information on the Cybersecurity Plan, please refer to Appendix C.

- **Cybersecurity Planning Committee Membership List**: The Cybersecurity Planning Committee should be seen as a platform to identify and then prioritize state-wide efforts, to include identifying opportunities to consolidate projects to increase efficiencies. Each eligible entity is required to submit confirmation that the committee is comprised of the required representatives. The eligible entity must also confirm that at least one-half of the representatives of the committee have professional experience relating to cybersecurity or information technology. For more information on the composition of the Cybersecurity Planning Committee, including how to leverage existing planning committees, please refer to Appendix B.
- **Cybersecurity Planning Committee Charter**: The Cybersecurity Planning Committee Charter must be submitted with the Cybersecurity Planning Committee Membership List attached as specified in Appendix B.
- **Cybersecurity Plan Submission Exception Request** (if applicable)
    - Applicants may request an exception to submitting their Cybersecurity Plan at the time of application. The exception request must be supported by the Chief Information Officer (CIO), Chief Information Security Office (CISO), or equivalent official.
    - If an exception is requested, SLCGP funds can only initially be used for activities that are integral to the development of the Cybersecurity Plan or are necessary to assist with activities that address imminent cybersecurity threats. Activities integral to the development of a Cybersecurity Plan are limited to investments and projects aligned to Objective 1 and Objective 2. Activities to address imminent cybersecurity threats are limited to investments and projects aligned to Objective 3.
    - **The eligible entity must also include a certification**, either as a separate document or as part of the applicable IJ(s), that all activities funded by the grant are integral to the development of the Cybersecurity Plan or are necessary to assist with activities that address imminent cybersecurity threats, as confirmed by the Secretary, acting through the CISA Director, to the information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity. If grant funding is necessary to assist with activities that address imminent cybersecurity threats, then that should be noted on the applicable IJ.
    - Recipients seeking funding to develop a Cybersecurity Plan must still submit IJs for Objectives 1, 2, and 3, noting that they will need to be updated once the Cybersecurity Plan is completed and approved. It is still optional to submit an IJ for Objective 4.
    - Once the Cybersecurity Plan is completed and approved by the Cybersecurity Planning Committee and CIO, CISO, or equivalent official, the applicant must then submit updated IJs for Objectives 1, 2, and 3, along with an updated IJ for Objective 4 if one was previously submitted, to DHS with the approved Cybersecurity Plan by September 30, 2023.

The following is required to request an exception:

- Statement from the applicant as to why they do not have an approved Cybersecurity

Plan;
- High-level plan, including dates and milestones, for completing and submitting the Plan to DHS; and
- Signatures of support from the eligible entity and CIO, CISO, or equivalent official.

11. Intergovernmental Review

An intergovernmental review may be required. Applicants must contact their state's Single Point of Contact (SPOC) to comply with the state's process under Executive Order 12372 (See https://www.archives.gov/federal-register/codification/executive-order/12372.html; https://www.whitehouse.gov/wp-content/uploads/2020/04/SPOC-4-13-20.pdf).

12. Funding Restrictions and Allowable Costs

All costs charged to awards covered by this NOFO must comply with the Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200, unless otherwise indicated in the NOFO or the terms and conditions of the award. This includes, among other requirements, that costs must be incurred, and products and services must be delivered, within the period of performance of the award. *See* 2 C.F.R. § 200.403(h) (referring to budget periods, which for DHS awards under this program is the same as the period of performance).

In general, the Cost Principles establish standards for the allowability of costs, provide detailed guidance on the cost accounting treatment of costs as direct or administrative costs, and set forth allowability principles for selected items of cost. More specifically, except as otherwise stated in this NOFO, the terms and condition of an award, or other program materials, costs charged to awards covered by this NOFO must be consistent with the Cost Principles for Federal Awards located at 2 C.F.R. Part 200, Subpart E. In order to be allowable, all costs charged to a DHS award or applied to the cost share must be reasonable in nature and amount and allocable to the particular DHS award.

Additionally, all costs charged to awards must comply with the grant program's applicable statutes, policies, requirements in this NOFO as well as with the terms and conditions of the award. If DHS staff identify costs that are inconsistent with any of these requirements, these costs may be disallowed, and DHS may recover funds as appropriate, consistent with applicable laws, regulations, and policies.

As part of these requirements, grant recipients and subrecipients may only use federal funds or funds applied to a cost share for the purposes set forth in this NOFO and the terms and conditions of the award, and those costs must be consistent with the statutory authority for the award.

Grant funds may not be used for matching funds for other federal grants/cooperative agreements, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the federal government or any other government entity.

Specific investments made in support of the funding priorities discussed in this NOFO generally fall into one of the following seven allowable expense categories:

- Planning;
- Equipment;
- Exercises;
- Management & Administration (M&A);
- Organization; and
- Training.

In addition, any entity that receives FY 2022 SLCGP funding may not use 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 SLT has previously used SLT funds to support the same or similar uses;
- For any recipient cost-sharing contribution;
- To pay a ransom;
- For recreational or social purposes;
- To pay for cybersecurity insurance premiums;
- To acquire land or to construct, remodel, or perform alternations of buildings or other physical facilities; or
- 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 or a local government within the jurisdiction of the eligible entity.

a. ***Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services***

Recipients and subrecipients of FEMA federal financial assistance are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA), Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200. Beginning August 13, 2020, the statute – as it applies to FEMA recipients, subrecipients, and their contractors and subcontractors – prohibits obligating or expending federal award funds on certain telecommunications and video surveillance products and contracting with certain entities for national security reasons.

Guidance is available at FEMA Policy #405-143-1: Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services or superseding document.

Additional guidance is available at Contract Provisions Guide: Navigating Appendix II to Part 200 - Contract Provisions for Non-Federal Entity Contracts Under Federal Awards.

Effective August 13, 2020, FEMA recipients and subrecipients **may not** use any FEMA funds under open or new awards to:

(1) Procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system;

(2) Enter into, extend, or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system; or

(3) Enter into, extend, or renew contracts with entities that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

I. REPLACEMENT EQUIPMENT AND SERVICES

FEMA grant funding may be permitted to procure replacement equipment and services impacted by this prohibition, provided the costs are otherwise consistent with the requirements of the NOFO.

II. DEFINITIONS

Per section 889(f)(2)-(3) of the FY 2019 NDAA and 2 C.F.R. § 200.216, covered telecommunications equipment or services means:

i. Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, (or any subsidiary or affiliate of such entities);
ii. For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
iii. Telecommunications or video surveillance services provided by such entities or using such equipment; or
iv. Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the People's Republic of China.

Examples of the types of products covered by this prohibition include phones, internet, video surveillance, and cloud servers when produced, provided, or used by the entities listed in the definition of "covered telecommunications equipment or services." *See* 2 C.F.R. § 200.471.

b. *Pre-Award Costs*

Pre-award costs are allowable only with the prior written approval of DHS/FEMA and as included in the award agreement. To request pre-award costs, a written request must be included with the application, signed by the AOR of the entity. The letter must outline what the pre-award costs are for, including a detailed budget break-out of pre-award costs from the post-award costs, and a justification for approval.

c. ***Management and Administration (M&A) Costs***

Management and administration (M&A) activities are allowable under this program. M&A activities are those directly relating to the management and administration of SLCGP funds, such as financial management and monitoring. A maximum of up to five percent of SLCGP funds awarded may be retained by the state, and any funds retained are to be used solely for M&A purposes associated with the SLCGP award.

Subrecipients may also retain a maximum of up to five percent of the funding passed through by the state solely for M&A purposes associated with the SLCGP award.

While the eligible entity may retain up to five percent of this total for M&A, the state must still ensure that all subrecipient award amounts meet the mandatory minimum pass-through requirements that are applicable to SLCGP. To meet this requirement, the percentage of funds passed through to local or tribal jurisdictions must be based on the state's total SLCGP award prior to withholding any M&A.

d. ***Indirect Facilities & Administrative (F&A) Costs***

Indirect costs are allowable under this program as described in 2 C.F.R. Part 200, including 2 C.F.R. § 200.414. Applicants with a current negotiated indirect cost rate agreement that desire to charge indirect costs to an award must provide a copy of their negotiated indirect cost rate agreement at the time of application. Not all applicants are required to have a current negotiated indirect cost rate agreement. Applicants that are not required by 2 C.F.R. Part 200 to have a negotiated indirect cost rate agreement but are required by 2 C.F.R. Part 200 to develop an indirect cost rate proposal must provide a copy of their proposal at the time of application. Applicants who do not have a current negotiated indirect cost rate agreement (including a provisional rate) and wish to charge the de minimis rate must reach out to the FEMA Grants Management Specialist for further instructions. Applicants who wish to use a cost allocation plan in lieu of an indirect cost rate must also reach out to the FEMA Grants Management Specialist for further instructions. Post-award requests to charge indirect costs will be considered on a case-by-case basis and based upon the submission of an agreement or proposal as discussed above or based upon on the de minimis rate or cost allocation plan, as applicable.

e. ***Other Direct Costs***

Funding guidelines established within this section support the development, updating, and implementing a cybersecurity plan. Allowable investments made in support of this goal must fall into the categories of planning, organization, exercises, training, or equipment, aligned to closing capability gaps or sustaining capabilities.

I. 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 and Cybersecurity Planning Committee requirements.

II. ORGANIZATION

Organization costs are allowable under this program. States must justify proposed expenditures of SLCGP funds to support organization activities within their IJ submission. Organizational activities include:

- Program management;
- Development of whole community partnerships that support the Cybersecurity Planning Committee;
- 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. The grant recipient must demonstrate that the personnel will be sustainable.

III. EQUIPMENT

Equipment costs are allowable under this program. SLCGP equipment is intended to be used to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state and local governments.

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. 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.

SLCGP funds may be used to purchase maintenance contracts or agreements, warranty coverage, licenses, and user fees in support of a system or equipment. These contracts may exceed the period of performance if they are purchased incidental to the original purchase of the system or equipment as long as the original purchase of the system or equipment is consistent with that which is typically provided for, or available through, these types of agreements, warranties, or contracts. When purchasing a stand-alone warranty or extending an existing maintenance contract on an already-owned piece of equipment system, coverage purchased may not exceed the period of performance of the award used to purchase the maintenance agreement or warranty, and it may only cover equipment purchased with SLCGP funds or for equipment dedicated for SLCGP-related purposes. As with warranties and maintenance agreements, this extends to licenses and user fees as well.

The use of SLCGP grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable, unless otherwise noted. Except for maintenance

plans or extended warranties purchased incidental to the original purchase of the equipment, the period covered by maintenance or warranty plan must not exceed the POP of the specific grant funds used to purchase the plan or warranty.

IV. TRAINING

Training costs are allowable under this program. Allowable training-related costs under SLCGP include the establishment, support, conduct, and attendance of training and/or in conjunction with training by other federal agencies. Training conducted using SLCGP funds should align to the eligible entity's Cybersecurity Plan and address a performance gap identified through assessments and contribute to building a capability that will be evaluated through a formal exercise. Any training or training gaps, including training related to underserved communities that may be more impacted by disasters, including children, seniors, individuals with disabilities or access and functional needs, individuals with diverse culture and language use, individuals with lower economic capacity and other underserved populations, should be identified in an assessment and addressed in the eligible entity's training cycle. Recipients are encouraged to use existing training rather than developing new courses. When developing new courses, recipients are encouraged to apply the Analyze, Design, Develop, Implement, and Evaluate (ADDIE) model of instructional design.

Recipients are also encouraged to utilize FEMA's National Preparedness Course Catalog. Trainings include programs or courses developed for and delivered by institutions and organizations funded by FEMA. This includes the Center for Domestic Preparedness (CDP), the Emergency Management Institute (EMI), and FEMA's Training Partner Programs, including the Continuing Training Grants (CTG), the National Domestic Preparedness Consortium (NDPC), the Rural Domestic Preparedness Consortium (RDPC), and other partners.

The catalog features a wide range of course topics in multiple delivery modes to meet FEMA's mission scope as well as the increasing training needs of federal, state, local, territorial, and tribal audiences. The catalog can be accessed at http://www.firstrespondertraining.gov.

Some training activities require Environmental and Historic Preservation (EHP) Review, including exercises, drills, or trainings that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises. Additional information on training requirements and EHP review can be found online at https://www.fema.gov/media-library/assets/documents/90195.

V. 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). HSEEP guidance for exercise design, development, conduct, evaluation, and improvement planning is located at https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep.

Some exercise activities require EHP review, including exercises, drills, or trainings that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises. Additional information on training requirements and EHP review can be found online at https://www.fema.gov/media-library/assets/documents/90195.

E. Application Review Information

1. Application Evaluation Criteria

a. *Programmatic Criteria*

DHS/FEMA will evaluate the FY 2022 SLCGP applications for completeness and applicant eligibility. DHS/CISA will evaluate the FY 2022 SLCGP applications for adherence to programmatic guidelines, and anticipated effectiveness of the proposed investments. The review will include verification of the following elements:

- Establishment of and composition of the Planning Committee;
- Cybersecurity Plan(s) or request for exception; and
- Proposed projects that are consistent with the Cybersecurity Plan(s), or will be consistent with the Cybersecurity Plan if requesting a grant to develop a Plan, and SLCGP program objectives and requirements.

In addition to the above, DHS/CISA will evaluate whether proposed projects are: 1) both feasible and effective at reducing the risks for which the project was designed; and 2) able to be fully completed within the four-year period of performance. DHS will use the information provided in the application and after the submission of the first Program Performance Report (PPR) to determine the feasibility and effectiveness of a grant project.

b. *Financial Integrity Criteria*

Prior to making a federal award, FEMA is required by 31 U.S.C. § 3354, as enacted by the Payment Integrity Information Act of 2019, Pub. L. No. 116-117 (2020); 41 U.S.C. § 2313; and 2 C.F.R. § 200.206 to review information available through any Office of Management and Budget (OMB)-designated repositories of governmentwide eligibility qualification or financial integrity information, including whether the applicant is suspended or debarred. FEMA may also pose additional questions to the applicant to aid in conducting the pre-award risk review. Therefore, application evaluation criteria may include the following risk-based considerations of the applicant:

i. Financial stability.
ii. Quality of management systems and ability to meet management standards.
iii. History of performance in managing federal award.
iv. Reports and findings from audits.
v. Ability to effectively implement statutory, regulatory, or other requirements.

c. *Supplemental Financial Integrity Criteria and Review*

Prior to making a federal award where the anticipated total federal share will be greater than the simplified acquisition threshold, currently $250,000:

i. FEMA is required to review and consider any information about the applicant, including information on the applicant's immediate and highest-level owner,

subsidiaries, and predecessors, if applicable, that is in the designated integrity and performance system accessible through the System for Award Management (SAM), which is currently the Federal Awardee Performance and Integrity Information System (FAPIIS).

ii. An applicant, at its option, may review information in FAPIIS and comment on any information about itself that a federal awarding agency previously entered.

iii. FEMA will consider any comments by the applicant, in addition to the other information in FAPIIS, in making a judgment about the applicant's integrity, business ethics, and record of performance under federal awards when completing the review of risk posed by applicants as described in 2 C.F.R. § 200.206.

2. Review and Selection Process

FEMA will follow all applicable statutes, rules, and requirements and will take into consideration materials accompanying BIL and annual appropriations acts, such as the Joint Explanatory Statement, as appropriate, in reviewing and determining recipient eligibility.

All proposed investments will undergo a federal review by FEMA and CISA to verify compliance with all administrative and eligibility criteria identified in the NOFO. The federal review for compliance will be conducted by FEMA. FEMA will use a checklist to verify compliance with all administrative and eligibility criteria identified in the NOFO.

Applicants must demonstrate how investments support closing capability gaps or sustaining capabilities. DHS will review IJs at both the investment and project level. The following criteria will be applied to the review of projects:

- Clarity: Sufficient detail to understand what the project is intending to do with grant dollars. (Yes/No)
- Logical/Project Alignment: Alignment with the stated SLCGP objectives and the applicant's Cybersecurity Plan or with the development of a Cybersecurity Plan. (Yes/No)
- Reasonableness: Costs for the items/services outlined within the project description are reasonable. Execution within the period of performance is feasible. (Yes/No)

Projects rated as effective or promising are approved. If an exception request from the FY 2022 Cybersecurity Plan submission requirement was submitted, SLCGP funds can only initially be used for activities that are integral to the development of the Cybersecurity Plan or to assist with activities that address imminent cybersecurity threats. This is limited to investments and projects aligned to Objective 1 and Objective 2.

In addition, investments with emergency communications activities will be reviewed to verify compliance with SAFECOM Guidance. FEMA and CISA will coordinate directly with the recipient on any compliance concerns and will provide technical assistance as necessary to help ensure full compliance.

F. Federal Award Administration Information

1. Notice of Award

Before accepting the award, the AOR and recipient should carefully read the award package. The award package includes instructions on administering the grant award and the terms and conditions associated with responsibilities under federal awards. **Recipients must accept all conditions in this NOFO as well as any specific terms and conditions in the Notice of Award to receive an award under this program.**

Notification of award approval is made through the ND Grants system through an automatic electronic mail to the recipient's authorized official listed in the initial application. The recipient should follow the directions in the notification to confirm acceptance of the award.

Recipients must accept their awards no later than 60 days from the award date. The recipient shall notify FEMA of its intent to accept and proceed with work under the award or provide a notice of intent to decline through the ND Grants system. For instructions on how to accept or decline an award in the ND Grants system, please see the ND Grants Grant Recipient User Guide, which is available at https://www.fema.gov/grants/guidance-tools/non-disaster-grants-management-system along with other ND Grants materials.

Funds will remain on hold until the recipient accepts the award through the ND Grants system and all other conditions of the award have been satisfied or until the award is otherwise rescinded. Failure to accept a grant award within the 60-day timeframe may result in a loss of funds.

2. Pass-Through Requirements

a. *Generally*

The eligible entity or multi-entity group must pass through at least 80 percent of the federal funds provided under the grant to local governments, including rural areas, within the jurisdiction of the eligible entity or multi-entity group.

Four requirements must be met to pass-through grant funds:

- The eligible entity must make a firm written commitment to passing through grant funds or equivalent services to subrecipients;
- The eligible entity's commitment must be unconditional (i.e., no contingencies for the availability of eligible entity funds);
- There must be documentary evidence (i.e., award document, terms, and conditions) of the commitment; and
- The award terms must be communicated to the subrecipient.

The signatory authority of the eligible entity must certify in writing to DHS/FEMA that pass-through requirements have been met. A letter of intent (or equivalent) to distribute funds is not considered sufficient; after the funds have been distributed, the SAA must self-certify, on behalf of the state, that the pass-through requirements have been met.

b. *Rural Area Pass-Through*

As part of the local government pass through requirement, in obligating funds, items,

services, capabilities, or activities to local governments, each eligible entity or multi-entity group is required to pass through at least 25% of the federal funds provided under the grant to rural areas. Per the Homeland Security Act of 2002, a rural area is defined in 49 U.S.C. § 5302 as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce.

The eligible entity or multi-entity group may either pass through 25% of the federal funds provided under the grant; items, services, capabilities, or activities having a value of at least 25% of the federal funds provided under the grant; or grant funds combined with other items, services, capabilities, or activities that have a total value of at least 25% of the federal funds provided under the grant.

Because the pass-through to rural entities is part of the overall 80% pass-through requirement to local governments, the eligible entity or multi-entity must obtain the consent of local governments if intending to pass through items, services, capabilities, or activities to rural areas in lieu of funding in order to count that value as part of the overall 80% pass-through requirement. *See* 6 U.S.C. §665g(n)(2)(A)-(B).

The same four criteria for pass-through to local governments also applies to the pass-through to rural areas within those local governments.

c. ***Exceptions***

The local government pass-through requirement, including the rural area pass-through requirement, does not apply to:

- Grants awarded solely to support activities integral to the development or revision of the Cybersecurity Plan of the eligible entity; or
- The District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, the United States Virgin Islands, or a Tribal government.

d. ***Timing***

The eligible entity must pass-through at least 80% of the funds awarded under the SLCGP to local governments, including at least 25% to rural areas, within 45 calendar days of receipt of the funds. "Receipt of the funds" occurs either when the eligible entity accepts the award or 15 calendar days after the eligible entity receives notice of the award, whichever is earlier.

Eligible entities are sent notification of SLCGP awards via the ND Grants system. If an eligible entity accepts its award within 15 calendar days of receiving notice of the award in the ND Grants system, the 45-calendar days pass-through period will start on the date the eligible entity accepted the award. Should an eligible entity not accept the SLCGP award within 15 calendar days of receiving notice of the award in the ND Grants system, the 45-calendar days pass-through period will begin 15 calendar days after the award notification is sent to the eligible entity via the ND Grants system.

It is important to note that the period of performance start date does not directly affect the

start of the 45-calendar day pass-through period. For example, an eligible entity may receive notice of the SLCGP award on September 20, 2022, while the period of performance dates for that award are October 1, 2022, through September 30, 2025. In this example, the 45-day pass-through period will begin on the date the eligible entity accepts the SLCGP award or October 5, 2022 (15 calendar days after the eligible entity was notified of the award), whichever date occurs first. The period of performance start date of October 1, 2022 would not affect the timing of meeting the 45-calendar day pass-through requirement.

e. ***Other Guidance and Requirements for Passing Through Items, Services, Capabilities, or Activities in Lieu of Funding***

The signatory authority of the eligible entity must certify in writing to DHS/FEMA that pass-through requirements have been met. A letter of intent (or equivalent) to distribute funds is not considered sufficient.

If a state wishes to pass through items, services, capabilities, or activities on a state-wide basis to all local governments and rural areas in lieu of funding, DHS recommends consulting with applicable municipal, city, county, rural area, or other local government councils or associations within the state to gauge the level of interest in and obtain consent to receive these in lieu of funding. DHS also recommends including these councils or associations in the Cybersecurity Planning Committees. States should also inform local governments, including rural areas, that by signing up for state-wide items, services, capabilities, or activities, that they are providing consent to receive these in lieu of funding.

States must still engage individual local governments as applicable to obtain consent where the state wants to pass through items, services, capabilities, or activities to a particular local government or rural area in lieu of funding. Consent can be given at individual local or tribal units of government, and does not have to be for all local governments within the state. If an individual unit of government does not consent to having the state retain a portion of funding, then the state must still pass-through funding to that local government, provided that entity has an approved project as part of the approved Cybersecurity Plan to utilize the funds.

In order for the SAA to retain more than 20% of SLCGP funds, the following conditions must be met:

- Must be for expenditures made by the state on behalf of the local or tribal government; and
- Must have written consent of the local or tribal government, specifying the amount of funds to be retained and the intended use of funds.

In providing these in lieu of funding, states must still ensure they are passing through an amount equal to at least 80% of the federal funding to local governments, including at least 25% to rural areas, within 45 days. The letter certifying the pass-through requirements have been met must indicate whether the state is passing through items, services, capabilities, or activities in lieu of funding as well as identify the consent it obtained from local governments. These decisions must also be documented in accordance with the Cybersecurity Planning Committee's Charter. For further information on Cybersecurity

Planning Committee requirements, see Appendix B.

3. Administrative and National Policy Requirements
In addition to the requirements of in this section and in this NOFO, FEMA may place specific terms and conditions on individual awards in accordance with 2 C.F.R. Part 200.

a. *DHS Standard Terms and Conditions*
All successful applicants for DHS grant and cooperative agreements are required to comply with DHS Standard Terms and Conditions, which are available online at: DHS Standard Terms and Conditions.

The applicable DHS Standard Terms and Conditions will be those in effect at the time the award was made. What terms and conditions will apply for the award will be clearly stated in the award package at the time of award.

b. *Ensuring the Protection of Civil Rights*
As the Nation works towards achieving the National Preparedness Goal, it is important to continue to protect the civil rights of individuals. Recipients and subrecipients must carry out their programs and activities, including those related to the building, sustainment, and delivery of core capabilities, in a manner that respects and ensures the protection of civil rights for protected populations.

Federal civil rights statutes, such as Section 504 of the Rehabilitation Act of 1973 and Title VI of the Civil Rights Act of 1964, along with DHS and FEMA regulations, prohibit discrimination on the basis of race, color, national origin, sex, religion, age, disability, limited English proficiency, or economic status in connection with programs and activities receiving federal financial assistance from FEMA.

The DHS Standard Terms and Conditions include a fuller list of the civil rights provisions that apply to recipients. These terms and conditions can be found in the DHS Standard Terms and Conditions. Additional information on civil rights provisions is available at https://www.fema.gov/about/offices/equal-rights/civil-rights.

Monitoring and oversight requirements in connection with recipient compliance with federal civil rights laws are also authorized pursuant to 44 C.F.R. Part 7.

In accordance with civil rights laws and regulations, recipients and subrecipients must ensure the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment.

c. *Environmental Planning and Historic Preservation (EHP) Compliance*
As a federal agency, FEMA is required to consider the effects of its actions on the environment and historic properties to ensure that all activities and programs funded by FEMA, including grant-funded projects, comply with federal EHP laws, Executive Orders, regulations, and policies, as applicable.

All non-critical new construction or substantial improvement of structures in a Special Flood Hazard Area must, at a minimum, apply the flood elevations of the Federal Flood Risk Management Standard's Freeboard Value Approach unless doing so would cause the project to be unable to meet applicable program cost-effectiveness requirements. All other types of projects may choose to apply the flood elevations of the Federal Flood Risk Management Standard's Freeboard Value Approach. See Executive Order (EO) 14030, Climate-Related Financial Risk and FEMA Policy #-206-21-0003, Partial Implementation of the Federal Flood Risk Management Standard for Hazard Mitigation Assistance Programs (Interim).

Recipients and subrecipients proposing projects that have the potential to impact the environment, including, but not limited to, the construction of communication towers, modification or renovation of existing buildings, structures, and facilities, or new construction including replacement of facilities, must participate in the FEMA EHP review process. The EHP review process involves the submission of a detailed project description along with any supporting documentation requested by FEMA in order to determine whether the proposed project has the potential to impact environmental resources or historic properties.

In some cases, FEMA is also required to consult with other regulatory agencies and the public in order to complete the review process. Federal law requires EHP review to be completed before federal funds are released to carry out proposed projects. FEMA may not be able to fund projects that are not incompliance with applicable EHP laws, Executive Orders, regulations, and policies.

Executive Order (EO) 13985, Advancing Racial Equity and Support for Underserved Communities through the Federal Government, rearticulates and strengthens the environmental justice framework articulated in 1994 in EO 12898, Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations. Specifically, Section 1 of E.O. 13985 states that: "Affirmatively advancing equity, civil rights, racial justice, and equal opportunity is the responsibility of the whole of our Government. Because advancing equity requires a systemic approach to embedding fairness in decision-making processes, executive departments and agencies…must recognize and work to redress inequalities in their policies and programs that serve as barriers to equal opportunity."

Many projects funded by GPD's grant programs can have significant impacts on environmental justice. In particular, construction of buildings and other structures and construction of new communication towers may have disproportionately high and adverse effects on minority and low-income populations. FEMA acknowledges the important role that FEMA recipients and subrecipients play in advancing and achieving environmental justice by identifying low-income and minority populations within a proposed project's affected area as early as possible and taking steps to accommodate these interests.

For consistency with the Administration's policy, FEMA will review and evaluate potential projects for racial equity and justice concerns. If FEMA determines that a proposed project would have a disproportionately high and adverse effect on minority or low-income

populations, FEMA will consult with recipients and subrecipients to discuss the feasibility of revising the scope of work to avoid these adverse impacts, or otherwise applying mitigation measures to alleviate these effects. In addition, FEMA may work with other recipients and subrecipients to solicit public input on the proposed projects for a more informed decision-making process. To learn more about how FEMA environmental justice responsibilities might affect your project, go to https://www.fema.gov/fact-sheet/executive-order-12898-environmental-justice.

DHS and FEMA EHP policy is found in directives and instructions available on the FEMA.gov EHP page, the FEMA website page that includes documents regarding EHP responsibilities and program requirements, including implementation of the National Environmental Policy Act and other EHP regulations and Executive Orders.

The GPD EHP screening form is located at https://www.fema.gov/media-library/assets/documents/90195. Additionally, all recipients under this funding opportunity are required to comply with the FEMA GPD EHP Policy Guidance, FEMA Policy #108-023-1, available at https://www.fema.gov/media-library/assets/documents/85376.

d. ***SAFECOM Guidance Compliance***

All entities using SLCGP funding to support emergency communications investments are required to comply with the SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance). The SAFECOM Guidance provides current information on emergency communications policies, eligible costs, best practices, and technical standards for SLT recipients investing federal funds in emergency communications projects. It is also designed to promote and align with the National Emergency Communications Plan (NECP). Conformance with the SAFECOM Guidance helps ensure that federally funded investments are compatible, interoperable, resilient, and support national goals and objectives for improving emergency communications. Applicants should use the SAFECOM Guidance during planning, development, and implementation of emergency communications projects and in conjunction with other planning documents. Specifically, Appendix D of the SAFECOM Guidance contains compliance instructions for SLCGP grant recipients.

If an entity uses SLCGP funding to support emergency communications investments, the following requirements shall apply to all such grant-funded communications investments in support of the emergency communications priorities and recognized best practices:
The signatory authority for the eligible entity must certify in writing to DHS/FEMA their compliance with the SAFECOM Guidance. The certification letter should be coordinated with the Statewide Interoperability Coordinator (SWIC) for each state and must be uploaded to ND Grants at the time of the first Program Performance Report (PPR) submission.

e. Requirement for using CISA Services

As a condition of receiving SLCGP funding, the grant recipient is required to adhere to or sign up for the following services, sponsored by CISA and further described in Appendix G, upon award as part of the statutory requirements in developing, implementing, or revising a Cybersecurity Plan. Participation in these services and memberships are not required for submission and approval of a grant:

- Sign up for cyber hygiene services, specifically vulnerability scanning and web application scanning; and
- Complete the Nationwide Cybersecurity Review, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually thereafter.

Recipients and subrecipients are also encouraged to sign up for the other services and memberships identified in Appendix G.

4. Reporting

Recipients are required to submit various financial and programmatic reports as a condition of award acceptance. Future awards and funds drawdown may be withheld if these reports are delinquent.

a. *Financial Reporting Requirements*

I. FEDERAL FINANCIAL REPORT (FFR)

Recipients must report obligations and expenditures through the FFR form (SF-425) to FEMA on a quarterly basis through the FFR form (SF-425). Recipients may review the Federal Financial Reporting Form (FFR) (SF-425) at https://www.grants.gov/web/grants/forms/post-award-reporting-forms.html#sortby=1

Recipients must file the FFR electronically using the Payment and Reporting Systems (PARS).

II. FFR REPORTING PERIODS AND DUE DATES

An FFR must be submitted quarterly throughout the period of performance, including partial calendar quarters, as well as in periods where no grant award activity occurs. The final FFR is due within 120 calendar days after the end of the period of performance. Future awards and fund drawdowns may be withheld if these reports are delinquent, demonstrate lack of progress, or are insufficient in detail.

Except for the final FFR due at 120 days after the end of the period of performance for purposes of closeout, the following reporting periods and due dates apply for the FFR.

Reporting Period	Report Due Date
October 1 – December 31	January 30
January 1 – March 31	April 30
April 1 – June 30	July 30
July 1 – September 30	October 30

b. *Programmatic Performance Reporting Requirements*

I. PERFORMANCE PROGRESS REPORT (PPR)

Recipients are responsible for providing updated performance reports on an annual basis, consistent with the authorizing statute, as an attachment in ND Grants. The PPR should include a:

- Brief narrative of overall project(s) status;

- Summary of project expenditures;
- Description of any potential issues that may affect project completion; and
- Data collected for DHS performance measures.

Program Performance Reporting Periods and Due Dates
The annual PPR submission is due January 30 of each year to account for the previous calendar year.

c. *Closeout Reporting Requirements*

I. CLOSEOUT REPORTING

Within 120 calendar days after the end of the period of performance for the prime award or after an amendment has been issued to close out an award before the original period of performance ends, recipients must liquidate all financial obligations and must submit the following:

i. The final request for payment, if applicable;
ii. The final FFR (SF-425).;
iii. The final progress report detailing all accomplishments, including a narrative summary of the impact of those accomplishments throughout the period of performance; and
iv. Other documents required by this NOFO, terms and conditions of the award, or other DHS/FEMA guidance.

In addition, pass-through entities are responsible for closing out their subawards as described in 2 C.F.R. § 200.344; subrecipients are still required to submit closeout materials within 90 calendar days of the period of performance end date. When a subrecipient completes all closeout requirements, pass-through entities must promptly complete all closeout actions for subawards in time for the recipient to submit all necessary documentation and information to FEMA during the closeout of the prime award.

After the prime award closeout reports have been reviewed and approved by FEMA, a closeout notice will be completed to close out the grant. The notice will indicate the period of performance as closed, list any remaining funds that will be deobligated, and address the requirement of maintaining the grant records for at least three years from the date of the final FFR. The record retention period may be longer, such as due to an audit or litigation, for equipment or real property used beyond the period of performance, or due to other circumstances outlined in 2 C.F.R. § 200.334.

The recipient is responsible for refunding to FEMA any balances of unobligated cash that FEMA paid that are not authorized to be retained per 2 C.F.R. § 200.344(d).

II. ADMINISTRATIVE CLOSEOUT

Administrative closeout is a mechanism for FEMA to unilaterally move forward with closeout of an award using available award information in lieu of final reports from the recipient per 2 C.F.R. § 200.344(h)-(i). It is a last resort available to FEMA, and if FEMA needs to administratively close an award, this may negatively impact a recipient's ability to

obtain future funding. This mechanism can also require FEMA to make cash or cost adjustments and ineligible cost determinations based on the information it has, which may result in identifying a debt owed to FEMA by the recipient.

When a recipient is not responsive to FEMA's reasonable efforts to collect required reports needed to complete the standard closeout process, FEMA is required under 2 C.F.R. § 200.344(h) to start the administrative closeout process within the regulatory timeframe. FEMA will make at least three written attempts to collect required reports before initiating administrative closeout. If the recipient does not submit all required reports in accordance with 2 C.F.R. § 200.344, this NOFO, and the terms and conditions of the award, FEMA must proceed to administratively close the award with the information available within one year of the period of performance end date. Additionally, if the recipient does not submit all required reports within one year of the period of performance end date, per 2 C.F.R. § 200.344(i), FEMA must report in FAPIIS the recipient's material failure to comply with the terms and conditions of the award.

If FEMA administratively closes an award where no final FFR has been submitted, FEMA uses that administrative closeout date in lieu of the final FFR submission date as the start of the record retention period under 2 C.F.R. § 200.334.

In addition, if an award is administratively closed, FEMA may decide to impose remedies for noncompliance per 2 C.F.R. § 200.339, consider this information in reviewing future award applications, or apply special conditions to existing or future awards.

d. ***Additional Reporting Requirements***

i. DISCLOSING INFORMATION PER 2 C.F.R. § 180.335

This reporting requirement pertains to disclosing information related to government-wide suspension and debarment requirements. Before a recipient enters into a grant award with FEMA, the recipient must notify FEMA if it knows if it or any of the recipient's principals under the award fall under one or more of the four criteria listed at 2 C.F.R. § 180.335:

i. Are presently excluded or disqualified;
ii. Have been convicted within the preceding three years of any of the offenses listed in 2 C.F.R. § 180.800(a) or had a civil judgment rendered against it or any of the recipient's principals for one of those offenses within that time period;
iii. Are presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state or local) with commission of any of the offenses listed in 2 C.F.R. § 180.800(a); or
iv. Have had one or more public transactions (federal, state, or local) terminated within the preceding three years for cause or default.

At any time after accepting the award, if the recipient learns that it or any of its principals falls under one or more of the criteria listed at 2 C.F.R. § 180.335, the recipient must provide immediate written notice to FEMA in accordance with 2 C.F.R. § 180.350.

II. Reporting of Matters Related to Recipient Integrity and Performance

Per 2 C.F.R. Part 200, Appendix I § F.3, the additional post-award reporting requirements in 2 C.F.R. Part 200, Appendix XII may apply to applicants who, if upon becoming recipients, have a total value of currently active grants, cooperative agreements, and procurement contracts from all federal awarding agencies that exceeds $10,000,000 for any period of time during the period of performance of an award under this funding opportunity.

Recipients that meet these criteria must maintain current information reported in FAPIIS about civil, criminal, or administrative proceedings described in paragraph 2 of Appendix XII at the reporting frequency described in paragraph 4 of Appendix XII.

III. Single Audit Report

For audits of fiscal years beginning on or after December 26, 2014, recipients that expend $750,000 or more from all federal funding sources during their fiscal year are required to submit an organization-wide financial and compliance audit report, also known as the single audit report.

The audit must be performed in accordance with the requirements of U.S. Government Accountability Office's (GAO) Government Auditing Standards, located at https://www.gao.gov/yellowbook/overview, and the requirements of Subpart F of 2 C.F.R. Part 200, located at http://www.ecfr.gov/cgi-bin/text-idx?node=sp2.1.200.f.

5. Program Evaluation

Recipients and subrecipients are encouraged to incorporate program evaluation activities from the outset of their program design and implementation to meaningfully document and measure their progress towards the outcomes proposed. Title I of the Foundations for Evidence-Based Policymaking Act of 2018 (Evidence Act), Pub. L. No. 115-435 (2019) defines evaluation as "an assessment using systematic data collection and analysis of one or more programs, policies, and organizations intended to assess their effectiveness and efficiency." Evidence Act § 101 (codified at 5 U.S.C. § 311). Credible program evaluation activities are implemented with relevance and utility, rigor, independence and objectivity, transparency, and ethics (OMB Circular A-11, Part 6 Section 290).

Evaluation costs are allowable costs (either as direct or indirect), unless prohibited by statute or regulation, and such costs may include the personnel and equipment needed for data infrastructure and expertise in data analysis, performance, and evaluation. (2 C.F.R. § 200).

In addition, recipients are required to participate in a DHS-led evaluation if selected, which may be carried out by a third-party on behalf of the Program Office or DHS. By accepting grant funds, recipients agree to participate in the evaluation, which may include analysis of individuals who benefit from the grant, and provide access to program operating personnel and participants, as specified by the evaluator(s) for six months after the period of performance.

6. Monitoring and Oversight

Per 2 C.F.R. § 200.337, DHS, through its authorized representatives, has the right, at all reasonable times, to make site visits or conduct desk reviews to review project accomplishments and management control systems to review award progress and to provide any required technical assistance, in the form of one-on-one guidance from a combination of Regional or Headquarters FEMA and CISA Staff. During site visits or desk reviews, DHS will review recipients' files related to the award. As part of any monitoring and program evaluation activities, recipients must permit DHS, upon reasonable notice, to review grant-related records and to interview the organization's staff and contractors regarding the program. Recipients must respond in a timely and accurate manner to DHS requests for information relating to the award.

Effective monitoring and oversight help DHS ensure that recipients use grant funds for their intended purpose(s); verify that projects undertaken are consistent with approved plans; and ensure that recipients make adequate progress toward stated goals and objectives. Additionally, monitoring serves as the primary mechanism to ensure that recipients comply with applicable laws, rules, regulations, program guidance, and requirements. DHS regularly monitors all grant programs both financially and programmatically in accordance with federal laws, regulations (including 2 C.F.R. Part 200), program guidance, and the terms and conditions of the award. All monitoring efforts ultimately serve to evaluate progress towards grant goals and proactively target and address issues that may threaten grant success during the period of performance. If the monitoring results in a determination that basic, minimum requirements as outlined in this NOFO are not being met, DHS may require corrective actions and/or initiate termination of the award.

DHS staff will periodically monitor recipients to ensure that administrative processes, policies and procedures, budgets, and other related award criteria are meeting Federal Government-wide and DHS regulations. Aside from reviewing quarterly financial and annual programmatic reports, DHS may also conduct enhanced monitoring through either desk-based reviews, onsite monitoring visits, or both. Enhanced monitoring will involve the review and analysis of the financial compliance and administrative processes, policies, activities, and other attributes of each federal assistance award, and it will identify areas where the recipient may need technical assistance, corrective actions, or other support.

Financial and programmatic monitoring are complementary processes within DHS's overarching monitoring strategy that function together to ensure effective grants management, accountability, and transparency; validate progress against grant and program goals; and safeguard federal funds against fraud, waste, and abuse. Financial monitoring primarily focuses on statutory and regulatory compliance with administrative grant requirements, while programmatic monitoring seeks to validate and assist in grant progress, targeting issues that may be hindering achievement of project goals and ensuring compliance with the purpose of the grant and grant program. Both monitoring processes are similar in that they feature initial reviews of all open awards, and additional, in-depth monitoring of grants requiring additional attention.

Recipients and subrecipients who are pass-through entities are responsible for monitoring their subrecipients in a manner consistent with the terms of the federal award at 2 C.F.R. Part 200, including 2 C.F.R. § 200.332. This includes the pass-through entity's responsibility to monitor the activities of the subrecipient as necessary to ensure that the subaward is used for authorized purposes, in compliance with federal statutes, regulations, and the terms and conditions of the subaward; and that subaward performance goals are achieved.
In terms of overall award management, recipient and subrecipient responsibilities include, but are not limited to: accounting of receipts and expenditures, cash management, maintaining adequate financial records, reporting and refunding expenditures disallowed by audits, monitoring if acting as a pass-through entity, or other assessments and reviews, and ensuring overall compliance with the terms and conditions of the award or subaward, as applicable, including the terms of 2 C.F.R. Part 200.

I. FINANCIAL MONITORING OVERVIEW AND APPROACH

FEMA's approach to financial monitoring provides a standard monitoring framework that promotes consistent processes across all monitoring staff. There are four core components of the monitoring process:

1. **Monitoring Assessment:** Monitoring staff measure each grant's monitoring needs using a system of pre-determined evaluation criteria. The criteria help assess the recipient and potential challenges to the success of the grant award.

2. **Monitoring Selection and Scheduling:** Monitoring staff make selection and scheduling decisions in accordance with applicable statutory requirements, such as the Homeland Security Act of 2002, as amended, and consider the results of the monitoring assessment process.

3. **Monitoring Activities:** Monitoring activities include cash analysis, desk reviews, and site visits. Grants Management Specialists are responsible for conducting quarterly or semi-annual reviews of all grants via cash analysis. Desk reviews and site visits are additional monitoring activities conducted on grants where the monitoring assessment process identified the need for additional monitoring and validated the use of FEMA resources for these activities.

4. **Post-Monitoring Actions:** Monitoring staff may follow up with recipients via post-monitoring actions based on the outcomes of monitoring activities. Post-monitoring actions include conducting additional monitoring; reviewing Corrective Action Plans (CAP) and monitoring the progress of CAP deliverables; documenting the resolution of identified corrective actions and issues; providing technical assistance and recipient training; and debt collection.

G. DHS Awarding Agency Contact Information

1. Contact and Resource Information

a. *Centralized Scheduling and Information Desk (CSID)*

CSID is a non-emergency comprehensive management and information resource developed by FEMA for grants stakeholders. CSID provides general information on all FEMA grant

programs and maintains a comprehensive database containing key personnel contact information at the federal, state, and local levels. When necessary, recipients will be directed to a federal point of contact who can answer specific programmatic questions or concerns. CSID can be reached by phone at (800) 368-6498 or by e-mail at askcsid@fema.dhs.gov, Monday through Friday, 9a.m. – 5 p.m. ET.

b. ***Grant Programs Directorate (GPD) Award Administration Division***
GPD's Award Administration Division (AAD) provides support regarding financial matters and budgetary technical assistance. Additional guidance and information can be obtained by contacting the AAD's Help Desk via e-mail at ASK-GMD@fema.dhs.gov.

c. ***Equal Rights***
The FEMA Office of Equal Rights (OER) is responsible for compliance with and enforcement of federal civil rights obligations in connection with programs and services conducted by FEMA and recipients of FEMA financial assistance. All inquiries and communications about federal civil rights compliance for FEMA grants under this NOFO should be sent to FEMA-CivilRightsOffice@fema.dhs.gov.

d. ***Environmental Planning and Historic Preservation***
GPD's EHP Team provides guidance and information about the EHP review process to recipients and subrecipients. All inquiries and communications about GPD projects under this NOFO or the EHP review process, including the submittal of EHP review materials, should be sent to gpdehpinfo@fema.dhs.gov.

2. Systems Information

a. ***Grants.gov***
For technical assistance with Grants.gov, call the customer support hotline 24 hours per day, 7 days per week (except federal holidays) at (800) 518-4726 or e-mail at support@grants.gov.

b. ***Non-Disaster (ND) Grants***
For technical assistance with the ND Grants system, please contact the ND Grants Helpdesk at ndgrants@fema.dhsgov or (800) 865-4076, Monday through Friday, 9 a.m. – 6 p.m. ET. User resources are available at https://www.fema.gov/grants/guidance-tools/non-disaster-grants-management-system

c. ***Payment and Reporting System (PARS)***
FEMA uses the Payment and Reporting System (PARS) for financial reporting, invoicing, and tracking payments. FEMA uses the Direct Deposit/Electronic Funds Transfer (DD/EFT) method of payment to recipients. To enroll in the DD/EFT, recipients must complete a Standard Form 1199A, Direct Deposit Form. If you have questions about the online system, please call the Customer Service Center at (866) 927-5646 or email ask-GMD@fema.dhs.gov.

H. Additional Information

1. Termination Provisions

FEMA may terminate a federal award in whole or in part for one of the following reasons. FEMA and the recipient must still comply with closeout requirements at 2 C.F.R. §§ 200.344-200.345 even if an award is terminated in whole or in part. To the extent that subawards are permitted under this NOFO, pass-through entities should refer to 2 C.F.R. § 200.340 for additional information on termination regarding subawards.

a. ***Noncompliance***

If a recipient fails to comply with the terms and conditions of a federal award, FEMA may terminate the award in whole or in part. If the noncompliance can be corrected, FEMA may first attempt to direct the recipient to correct the noncompliance. This may take the form of a Compliance Notification. If the noncompliance cannot be corrected or the recipient is non-responsive, FEMA may proceed with a Remedy Notification, which could impose a remedy for noncompliance per 2 C.F.R. § 200.339, including termination. Any action to terminate based on noncompliance will follow the requirements of 2 C.F.R. §§ 200.341-200.342 as well as the requirement of 2 C.F.R. § 200.340(c) to report in FAPIIS the recipient's material failure to comply with the award terms and conditions. See also the section on Actions to Address Noncompliance in this NOFO.

b. ***With the Consent of the Recipient***

FEMA may also terminate an award in whole or in part with the consent of the recipient, in which case the parties must agree upon the termination conditions, including the effective date, and in the case of partial termination, the portion to be terminated.

c. ***Notification by the Recipient***

The recipient may terminate the award, in whole or in part, by sending written notification to FEMA setting forth the reasons for such termination, the effective date, and in the case of partial termination, the portion to be terminated. In the case of partial termination, FEMA may determine that a partially terminated award will not accomplish the purpose of the federal award, so FEMA may terminate the award in its entirety. If that occurs, FEMA will follow the requirements of 2 C.F.R. §§ 200.341-200.342 in deciding to fully terminate the award.

2. Period of Performance Extensions

Extensions to the period of performance for this program are allowed. Extensions to the period of performance identified in the award will only be considered through formal, written requests to FEMA and must contain specific and compelling justifications as to why an extension is required. Recipients are advised to coordinate with FEMA and CISA, as needed, when preparing an extension request.

All extension requests must address the following:

a. The grant program, fiscal year, and award number;
b. Reason for the delay –including details of the legal, policy, or operational challenges that prevent the final outlay of awarded funds by the deadline;
c. Current status of the activity(ies);

d. Approved period of performance termination date and new project completion date;
e. Amount of funds drawn down to date;
f. Remaining available funds, both federal and, if applicable, non-federal;
g. Budget outlining how remaining federal and, if applicable, non-federal funds will be expended;
h. Plan for completion, including milestones and timeframes for achieving each milestone and the position or person responsible for implementing the plan for completion; and
i. Certification that the activity(ies) will be completed within the extended period of performance without any modification to the original statement of work, as described in the investment justification and as approved by DHS.

Extension requests will be granted only due to compelling legal, policy, or operational challenges. Extension requests will only be considered for the following reasons:

- Contractual commitments by the recipient or subrecipient with vendors prevent completion of the project, including delivery of equipment or services, within the existing period of performance;
- The project must undergo a complex environmental review that cannot be completed within the existing period of performance;
- Projects are long-term by design, and therefore acceleration would compromise core programmatic goals; or
- Where other special or extenuating circumstances exist.

Recipients should submit all proposed extension requests to DHS for review and approval at least 120 days prior to the end of the period of performance to allow sufficient processing time. Extensions are typically granted for no more than a six-month period.

3. Disability Integration

Pursuant to Section 504 of the Rehabilitation Act of 1973, recipients of FEMA financial assistance must ensure that their programs and activities do not discriminate against other qualified individuals with disabilities.

Grant recipients should engage with the whole community to advance individual and community preparedness and to work as a nation to build and sustain resilience. In doing so, recipients are encouraged to consider the needs of individuals with disabilities into the activities and projects funded by the grant.

DHS expects that the integration of the needs of people with disabilities will occur at all levels, including planning; alerting, notification, and public outreach; training; purchasing of equipment and supplies; protective action implementation; and exercises/drills.

The following are examples that demonstrate the integration of the needs of people with disabilities in carrying out FEMA awards under this program:

- Include representatives of organizations that work with/for people with disabilities on planning committees, work groups and other bodies engaged in development and implementation of the grant programs and activities.
- Hold all activities related to the grant in locations that are accessible to persons with physical disabilities to the extent practicable.

- Acquire language translation services, including American Sign Language, that provide public information across the community and in shelters.
- Ensure shelter-specific grant funds are in alignment with FEMA's Guidance on Planning for Integration of Functional Needs Support Services in General Population Shelters.
- If making alterations to an existing building to a primary function area utilizing federal funds, complying with the most recent codes and standards and making path of travel to the primary function area accessible to the greatest extent possible.
- Implement specific procedures used by public transportation agencies that include evacuation and passenger communication plans and measures for individuals with disabilities.
- Identify, create, and deliver training to address any training gaps specifically aimed toward whole-community preparedness. Include and interact with individuals with disabilities, aligning with the designated program capability.
- Establish best practices in inclusive planning and preparedness that consider physical access, language access, and information access. Examples of effective communication access include providing auxiliary aids and services such as sign language interpreters, Computer Aided Real-time Translation (CART), and materials in Braille or alternate formats.

FEMA grant recipients can fund projects towards the resilience of the whole community, including people with disabilities, such as training, outreach and safety campaigns, provided that the project aligns with this NOFO and the terms and conditions of the award.

4. Conflicts of Interest in the Administration of Federal Awards or Subawards

For conflicts of interest under grant-funded procurements and contracts, refer to the section on Procurement Integrity in this NOFO and 2 C.F.R. §§ 200.317 – 200.327.

To eliminate and reduce the impact of conflicts of interest in the subaward process, recipients and pass-through entities must follow their own policies and procedures regarding the elimination or reduction of conflicts of interest when making subawards. Recipients and pass-through entities are also required to follow any applicable federal and SLT statutes or regulations governing conflicts of interest in the making of subawards.

The recipient or pass-through entity must disclose to the respective Preparedness Officer or Program Manager, in writing, any real or potential conflict of interest that may arise during the administration of the federal award, as defined by the federal or SLT statutes or regulations or their own existing policies, within five days of learning of the conflict of interest. Similarly, subrecipients, whether acting as subrecipients or as pass-through entities, must disclose any real or potential conflict of interest to the recipient or next-level pass-through entity as required by the recipient or pass-through entity's conflict of interest policies, or any applicable federal or SLT statutes or regulations.

Conflicts of interest may arise during the process of DHS making a federal award in situations where an employee, officer, or agent, any members of his or her immediate family,

his or her partner has a close personal relationship, a business relationship, or a professional relationship, with an applicant, subapplicant, recipient, subrecipient, or DHS employees.

5. Procurement Integrity

Through audits conducted by the DHS Office of Inspector General (OIG) and FEMA grant monitoring, findings have shown that some FEMA recipients have not fully adhered to the proper procurement requirements at 2 C.F.R. §§ 200.317 – 200.327 when spending grant funds. Anything less than full compliance with federal procurement requirements jeopardizes the integrity of the grant as well as the grant program. To assist with determining whether an action is a procurement or instead a subaward, please consult 2 C.F.R. § 200.331. For detailed guidance on the federal procurement standards, recipients and subrecipients should refer to various materials issued by FEMA's Procurement Disaster Assistance Team (PDAT), such as the PDAT Field Manual and Contract Provisions Guide. Additional resources, including an upcoming trainings schedule can be found on the PDAT Website: https://www.fema.gov/grants/procurement.

The below highlights the federal procurement requirements for FEMA recipients when procuring goods and services with federal grant funds. FEMA will include a review of recipients' procurement practices as part of the normal monitoring activities. **All procurement activity must be conducted in accordance with federal procurement standards at 2 C.F.R. §§ 200.317 – 200.327.** Select requirements under these standards are listed below. The recipient and any of its subrecipients must comply with all requirements, even if they are not listed below.

Under 2 C.F.R. § 200.317, when procuring property and services under a federal award, states (including territories) must follow the same policies and procedures they use for procurements from their non-federal funds; additionally, states must now follow 2 C.F.R. § 200.321 regarding socioeconomic steps, 200.322 regarding domestic preferences for procurements, 200.323 regarding procurement of recovered materials, and 2 C.F.R. § 200.327 regarding required contract provisions.

All other non-federal entities, such as tribes (collectively, non-state entities), must have and use their own documented procurement procedures that reflect applicable SLT laws and regulations, provided that the procurements conform to applicable federal law and the standards identified in 2 C.F.R. Part 200. These standards include, but are not limited to, providing for full and open competition consistent with the standards of 2 C.F.R. § 200.319 and the required procurement methods at § 200.320.

a. *Important Changes to Procurement Standards in 2 C.F.R. Part 200*

OMB recently updated various parts of Title 2 of the Code of Federal Regulations, among them, the procurement standards. States are now required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. § 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States per 2 C.F.R. § 200.322. More

information on OMB's revisions to the federal procurement standards can be found in Purchasing Under a FEMA Award: OMB Revisions Fact Sheet.

The recognized procurement methods in 2 C.F.R. § 200.320 have been reorganized into informal procurement methods, which include micro-purchases and small purchases; formal procurement methods, which include sealed bidding and competitive proposals; and noncompetitive procurements. The federal micro-purchase threshold is currently $10,000, and non-state entities may use a lower threshold when using micro-purchase procedures under a FEMA award. If a non-state entity wants to use a micro-purchase threshold higher than the federal threshold, it must follow the requirements of 2 C.F.R. § 200.320(a)(1)(iii)-(v). The federal simplified acquisition threshold is currently $250,000, and a non-state entity may use a lower threshold but may not exceed the federal threshold when using small purchase procedures under a FEMA award. *See* 2 C.F.R. § 200.1 (citing the definition of simplified acquisition threshold from 48 C.F.R. Part 2, Subpart 2.1).

See 2 C.F.R. §§ 200.216, 200.471, and Appendix II as well as section D.13.a of the NOFO regarding prohibitions on covered telecommunications equipment or services.

b. ***Competition and Conflicts of Interest***

Among the requirements of 2 C.F.R. § 200.319(b) applicable to all non-federal entities other than states, in order to ensure objective contractor performance and eliminate unfair competitive advantage, contractors that develop or draft specifications, requirements, statements of work, or invitations for bids or requests for proposals must be excluded from competing for such procurements. FEMA considers these actions to be an organizational conflict of interest and interprets this restriction as applying to contractors that help a non-federal entity develop its grant application, project plans, or project budget. This prohibition also applies to the use of former employees to manage the grant or carry out a contract when those former employees worked on such activities while they were employees of the non-federal entity.

Under this prohibition, unless the non-federal entity solicits for and awards a contract covering both development and execution of specifications (or similar elements as described above), and this contract was procured in compliance with 2 C.F.R. §§ 200.317 – 200.327, federal funds cannot be used to pay a contractor to carry out the work if that contractor also worked on the development of those specifications. This rule applies to all contracts funded with federal grant funds, including pre-award costs, such as grant writer fees, as well as post-award costs, such as grant management fees.

Additionally, some of the situations considered to be restrictive of competition include, but are not limited to:

- Placing unreasonable requirements on firms for them to qualify to do business;
- Requiring unnecessary experience and excessive bonding;
- Noncompetitive pricing practices between firms or between affiliated companies;
- Noncompetitive contracts to consultants that are on retainer contracts;
- Organizational conflicts of interest;

- Specifying only a "brand name" product instead of allowing "an equal" product to be offered and describing the performance or other relevant requirements of the procurement; and
- Any arbitrary action in the procurement process.

Per 2 C.F.R. § 200.319(c), non-federal entities other than states must conduct procurements in a manner that prohibits the use of statutorily or administratively imposed SLT geographical preferences in the evaluation of bids or proposals, except in those cases where applicable federal statutes expressly mandate or encourage geographic preference. Nothing in this section preempts state licensing laws. When contracting for architectural and engineering services, geographic location may be a selection criterion provided its application leaves an appropriate number of qualified firms, given the nature and size of the project, to compete for the contract.

Under 2 C.F.R. § 200.318(c)(1), non-federal entities other than states are required to maintain written standards of conduct covering conflicts of interest and governing the actions of their employees engaged in the selection, award, and administration of contracts. **No employee, officer, or agent may participate in the selection, award, or administration of a contract supported by a federal award if he or she has a real or apparent conflict of interest.** Such conflicts of interest would arise when the employee, officer or agent, any member of his or her immediate family, his or her partner, or an organization that employs or is about to employ any of the parties indicated herein, has a financial or other interest in or a tangible personal benefit from a firm considered for a contract. The officers, employees, and agents of the non-federal entity may neither solicit nor accept gratuities, favors, or anything of monetary value from contractors or parties to subcontracts. However, non-federal entities may set standards for situations in which the financial interest is not substantial, or the gift is an unsolicited item of nominal value. The standards of conduct must provide for disciplinary actions to be applied for violations of such standards by officers, employees, or agents of the non-federal entity.

Under 2 C.F.R. 200.318(c)(2), if the recipient or subrecipient (other than states) has a parent, affiliate, or subsidiary organization that is not a state, local, tribal, or territorial government, the non-federal entity must also maintain written standards of conduct covering organizational conflicts of interest. In this context, organizational conflict of interest means that because of a relationship with a parent company, affiliate, or subsidiary organization, the non-federal entity is unable or appears to be unable to be impartial in conducting a procurement action involving a related organization. The non-federal entity must disclose in writing any potential conflicts of interest to FEMA or the pass-through entity in accordance with applicable FEMA policy.

c. ***Supply Schedules and Purchasing Programs***

Generally, a non-federal entity may seek to procure goods or services from a federal supply schedule, state supply schedule, or group purchasing agreement.

I. General Services Administration Schedules

States, tribes, and local governments, and any instrumentality thereof (such as local education agencies or institutions of higher education) may procure goods and services from a General Services Administration (GSA) schedule. GSA offers multiple efficient and effective procurement programs for state, tribal, and local governments, and instrumentalities thereof, to purchase products and services directly from pre-vetted contractors. The GSA Schedules (also referred to as the Multiple Award Schedules and the Federal Supply Schedules) are long-term government-wide contracts with commercial firms that provide access to millions of commercial products and services at volume discount pricing.

Information about GSA programs for states, tribes, and local governments, and instrumentalities thereof, can be found at https://www.gsa.gov/resources-for/programs-for-State-and-local-governments and https://www.gsa.gov/buying-selling/purchasing-programs/gsa-schedules/schedule-buyers/state-and-local-governments.

For tribes, local governments, and their instrumentalities that purchase off of a GSA schedule, this will satisfy the federal requirements for full and open competition provided that the recipient follows the GSA ordering procedures; however, tribes, local governments, and their instrumentalities will still need to follow the other rules under 2 C.F.R. §§ 200.317 – 200.327, such as solicitation of minority businesses, women's business enterprises, small businesses, or labor surplus area firms (§ 200.321), domestic preferences (§ 200.322), contract cost and price (§ 200.324), and required contract provisions (§ 200.327 and Appendix II).

II. Other Supply Schedules and Programs

For non-federal entities other than states, such as tribes, local governments, and nonprofits, that want to procure goods or services from a state supply schedule, cooperative purchasing program, or other similar program, in order for such procurements to be permissible under federal requirements, the following must be true:

- The procurement of the original contract or purchasing schedule and its use by the non-federal entity complies with state and local law, regulations, and written procurement procedures;
- The state or other entity that originally procured the original contract or purchasing schedule entered into the contract or schedule with the express purpose of making it available to the non-federal entity and other similar types of entities;
- The contract or purchasing schedule specifically allows for such use, and the work to be performed for the non-federal entity falls within the scope of work under the contract as to type, amount, and geography;
- The procurement of the original contract or purchasing schedule complied with all the procurement standards applicable to a non-federal entity other than states under at 2 C.F.R. §§ 200.317 – 200.327; and
- With respect to the use of a purchasing schedule, the non-federal entity must follow ordering procedures that adhere to applicable state, tribal, and local laws and regulations and the minimum requirements of full and open competition under 2 C.F.R. Part 200.

If a non-federal entity other than a state seeks to use a state supply schedule, cooperative purchasing program, or other similar type of arrangement, FEMA recommends the recipient discuss the procurement plans with its FEMA Grants Management Specialist.

d. ***Procurement Documentation***

Per 2 C.F.R. § 200.318(i), non-federal entities other than states and territories are required to maintain and retain records sufficient to detail the history of procurement covering at least the rationale for the procurement method, selection of contract type, contractor selection or rejection, and the basis for the contract price. States and territories are encouraged to maintain and retain this information as well and are reminded that in order for any cost to be allowable, it must be adequately documented per 2 C.F.R. § 200.403(g).

Examples of the types of documents that would cover this information include but are not limited to:

- Solicitation documentation, such as requests for quotes, invitations for bids, or requests for proposals;
- Responses to solicitations, such as quotes, bids, or proposals;
- Pre-solicitation independent cost estimates and post-solicitation cost/price analyses on file for review by federal personnel, if applicable;
- Contract documents and amendments, including required contract provisions; and
- Other documents required by federal regulations applicable at the time a grant is awarded to a recipient.

Additional information on required procurement records can be found on pages 24-26 of the PDAT Field Manual.

6. Record Retention

a. ***Record Retention Period***

Financial records, supporting documents, statistical records, and all other non-federal entity records pertinent to a federal award generally must be maintained for at least three years from the date the final FFR is submitted. *See* 2 C.F.R. § 200.334. Further, if the recipient does not submit a final FFR and the award is administratively closed, FEMA uses the date of administrative closeout as the start of the general record retention period.

The record retention period **may be longer than three years or have a different start date** in certain cases. These include:

- Records for real property and equipment acquired with Federal funds must be retained for **three years after final disposition of the property**. *See* 2 C.F.R. § 200.334(c).
- If any litigation, claim, or audit is started before the expiration of the three-year period, the records **must be retained until** all litigation, claims, or audit findings involving the records **have been resolved and final action taken**. *See* 2 C.F.R. § 200.334(a).
- The **record retention period will be extended if the non-federal entity is notified in writing** of the extension by FEMA, the cognizant or oversight agency for audit, or the cognizant agency for indirect costs, or pass-through entity. *See* 2 C.F.R. § 200.334(b).

- Where FEMA requires recipients to report program income after the period of performance ends, the **program income record retention period begins at the end of the recipient's fiscal year in which program income is earned**. *See* 2 C.F.R. § 200.334(e).
- For indirect cost rate computations and proposals, cost allocation plans, or any similar accounting computations of the rate at which a particular group of costs is chargeable (such as computer usage chargeback rates or composite fringe benefit rates), the start of the record retention period depends on whether the indirect cost rate documents were submitted for negotiation. If the **indirect cost rate documents were submitted for negotiation, the record retention period begins from the date those documents were submitted** for negotiation. If indirect cost rate documents were **not submitted for negotiation, the record retention period begins at the end of the recipient's fiscal year or other accounting period covered by that indirect cost rate**. *See* 2 C.F.R. § 200.334(f).

b. ***Types of Records to Retain***

FEMA requires that non-federal entities maintain the following documentation for federally funded purchases:

- Specifications
- Solicitations
- Competitive quotes or proposals
- Basis for selection decisions
- Purchase orders
- Contracts
- Invoices
- Cancelled checks

Non-federal entities should keep detailed records of all transactions involving the grant. FEMA may at any time request copies of any relevant documentation and records, including purchasing documentation along with copies of cancelled checks for verification. *See, e.g.*, 2 C.F.R. §§ 200.318(i), 200.334, 200.337.

In order for any cost to be allowable, it must be adequately documented per 2 C.F.R. § 200.403(g). Non-federal entities who fail to fully document all purchases may find their expenditures questioned and subsequently disallowed.

7. Actions to Address Noncompliance

Non-federal entities receiving financial assistance funding from FEMA are required to comply with requirements in the terms and conditions of their awards or subawards, including the terms set forth in applicable federal statutes, regulations, NOFOs, and policies. Throughout the award lifecycle or even after an award has been closed, FEMA or the pass-through entity may discover potential or actual noncompliance on the part of a recipient or subrecipient. This potential or actual noncompliance may be discovered through routine monitoring, audits, closeout, or reporting from various sources.

In the case of any potential or actual noncompliance, FEMA may place special conditions on an award per 2 C.F.R. §§ 200.208 and 200.339, FEMA may place a hold on funds until the matter is corrected, or additional information is provided per 2 C.F.R. § 200.339, or it may do both. Similar remedies for noncompliance with certain federal civil rights laws are authorized pursuant to 44 C.F.R. Parts 7 and 19.

In the event the noncompliance is not able to be corrected by imposing additional conditions or the recipient or subrecipient refuses to correct the matter, FEMA might take other remedies allowed under 2 C.F.R. § 200.339. These remedies include actions to disallow costs, recover funds, wholly or partly suspend or terminate the award, initiate suspension and debarment proceedings, withhold further federal awards, or take other remedies that may be legally available. For further information on termination due to noncompliance, see the section on Termination Provisions in the NOFO.

FEMA may discover and take action on noncompliance even after an award has been closed. The closeout of an award does not affect FEMA's right to disallow costs and recover funds as long the action to disallow costs takes place during the record retention period. *See* 2 C.F.R. §§ 200.334, 200.345(a). Closeout also does not affect the obligation of the non-federal entity to return any funds due as a result of later refunds, corrections, or other transactions. 2 C.F.R. § 200.345(a)(2).

The types of funds FEMA might attempt to recover include, but are not limited to, improper payments, cost share reimbursements, program income, interest earned on advance payments, or equipment disposition amounts.

FEMA may seek to recover disallowed costs through a Notice of Potential Debt Letter, a Remedy Notification, or other letter. The document will describe the potential amount owed, the reason why FEMA is recovering the funds, the recipient's appeal rights, how the amount can be paid, and the consequences for not appealing or paying the amount by the deadline.

If the recipient neither appeals nor pays the amount by the deadline, the amount owed will become final. Potential consequences if the debt is not paid in full or otherwise resolved by the deadline include the assessment of interest, administrative fees, and penalty charges; administratively offsetting the debt against other payable federal funds; and transferring the debt to the U.S. Department of the Treasury for collection.

FEMA notes the following common areas of noncompliance for FEMA's grant programs:

- Insufficient documentation and lack of record retention;
- Failure to follow the procurement under grants requirements;
- Failure to submit closeout documents in a timely manner;
- Failure to follow EHP requirements; and
- Failure to comply with the POP deadline.

8. Audits

FEMA grant recipients are subject to audit oversight from multiple entities including the DHS OIG, the GAO, the pass-through entity, or independent auditing firms for single audits,

and may cover activities and costs incurred under the award. Auditing agencies such as the DHS OIG, the GAO, and the pass-through entity (if applicable), and FEMA in its oversight capacity, must have access to records pertaining to the FEMA award. Recipients and subrecipients must retain award documents for at least three years from the date the final FFR is submitted, and even longer in many cases subject to the requirements of 2 C.F.R. § 200.334. In the case of administrative closeout, documents must be retained for at least three years from the date of closeout, or longer subject to the requirements of 2 C.F.R. § 200.334. If documents are retained longer than the required retention period, the DHS OIG, the GAO, and the pass-through entity, as well as FEMA in its oversight capacity, have the right to access these records as well. *See* 2 C.F.R. §§ 200.334, 200.337.

Additionally, non-federal entities must comply with the single audit requirements at 2 C.F.R. Part 200, Subpart F. Specifically, non-federal entities, other than for-profit subrecipients, that expend $750,000 or more in federal awards during their fiscal year must have a single or program-specific audit conducted for that year in accordance with Subpart F. 2 C.F.R. § 200.501. A single audit covers all federal funds expended during a fiscal year, not just FEMA funds. The cost of audit services may be allowable per 2 C.F.R. § 200.425, but non-federal entities must select auditors in accordance with 2 C.F.R. § 200.509, including following the proper procurement procedures. For additional information on single audit reporting requirements, see section F of this NOFO under the header "Single Audit Report" within the subsection "Additional Reporting Requirements."

The objectives of single audits are to:

- Determine whether financial statements conform to generally accepted accounting principles (GAAP);
- Determine whether the schedule of expenditures of federal awards is presented fairly;
- Understand, assess, and test the adequacy of internal controls for compliance with major programs; and
- Determine whether the entity complied with applicable laws, regulations, and contracts or grants.

For single audits, the auditee is required to prepare financial statements reflecting its financial position, a schedule of federal award expenditures, and a summary of the status of prior audit findings and questioned costs. The auditee also is required to follow up and take appropriate corrective actions on new and previously issued but not yet addressed audit findings. The auditee must prepare a corrective action plan to address the new audit findings. 2 C.F.R. §§ 200.508, 200.510, 200.511.

Non-federal entities must have an audit conducted, either single or program-specific, of their financial statements and federal expenditures annually or biennially pursuant to 2 C.F.R. § 200.504. Non-federal entities must also follow the information submission requirements of 2 C.F.R. § 200.512, including submitting the audit information to the Federal Audit Clearinghouse within the earlier of 30 calendar days after receipt of the auditor's report(s) or nine months after the end of the audit period. The audit information to be submitted include the data collection form described at 2 C.F.R. § 200.512(c) and Appendix X to 2 C.F.R. Part 200 as well as the reporting package described at 2 C.F.R. § 200.512(b).

The non-federal entity must retain one copy of the data collection form and one copy of the reporting package for three years from the date of submission to the Federal Audit Clearinghouse. 2 C.F.R. § 200.512; *see also* 2 C.F.R. § 200.517 (setting requirements for retention of documents by the auditor and access to audit records in the auditor's possession).

FEMA, the DHS OIG, the GAO, and the pass-through entity (if applicable), as part of monitoring or as part of an audit, may review a non-federal entity's compliance with the single audit requirements. In cases of continued inability or unwillingness to have an audit conducted in compliance with 2 C.F.R. Part 200, Subpart F, FEMA and the pass-through entity, if applicable, are required to take appropriate remedial action under 2 C.F.R. § 200.339 for noncompliance, pursuant to 2 C.F.R. § 200.505.

9. Payment Information

FEMA uses the Direct Deposit/Electronic Funds Transfer (DD/EFT) method of payment to recipients. To enroll in the DD/EFT, the recipient must complete SF-1199A, Direct Deposit Form.

FEMA utilizes the Payment and Reporting System (PARS) for financial reporting, invoicing and tracking payments. For additional information, refer to https://isource.fema.gov/sf269/execute/LogIn?sawContentMessage=true.

10. Whole Community Preparedness

Preparedness is a shared responsibility that calls for the involvement of everyone—not just the government—in preparedness efforts. By working together, everyone can help keep the nation safe from harm and help keep it resilient when struck by hazards, such as natural disasters, acts of terrorism, and pandemics.

Whole Community includes:

- Individuals and families, including those with access and functional needs;
- Businesses;
- Faith-based and community organizations;
- Nonprofit groups;
- Schools and academia;
- Media outlets; and
- All levels of government, including state, local, tribal, territorial, and federal partners.

The phrase "Whole Community" or "Whole of Community" often appears in preparedness materials, as it is one of the guiding principles. It means:

1. Involving people in the development of national preparedness documents, and
2. Ensuring their roles and responsibilities are reflected in the content of the materials.

11. Continuity Capability

Continuity should be integrated into each core capability and the coordinating structures that provide them. Protection of critical systems and networks that ensure continuity of operation, business and government are fundamental to ensuring the delivery of all core capabilities. Continuity capabilities increase resilience and the probability that organizations can perform

essential functions in the delivery of core capabilities that support the mission areas. FEMA is responsible for developing, managing, and promulgating national continuity planning, guidance, training, and exercise programs for the whole community.

FEMA develops and promulgates directives, policy, and guidance for continuing SLT government jurisdictions, nongovernmental organizations, and private sector organizations' essential functions across a broad spectrum of emergencies. This direction and guidance assist in developing capabilities for continuing the essential functions of SLT governmental entities, as well as public/private critical infrastructure owners, operators, and regulators enabling them.

Continuity Guidance Circular outline continuity requirements for agencies and organizations and provide guidance, methodology, and checklists. For additional information on continuity programs, guidance, and directives, visit the Continuity Resource Toolkit at https://www.fema.gov/emergency-managers/national-preparedness/continuity/toolkit. For additional information on continuity programs, guidance, and directives, visit https://www.fema.gov/emergency-managers/national-preparedness/continuity.

This aligns with the requirements that Cybersecurity Plans ensure continuity of operations of the state or territory as well as applicable local governments in the event of a cybersecurity incident, as well as continuity of communications and data networks within the state or territory and between the state or territory and applicable local governments. 6 U.S.C. § 665g(e)(2)(B)(vii), (ix).

12. Appendices

Appendix A. Program Goals and Objectives
Appendix B. Cybersecurity Planning Committee
Appendix C. Cybersecurity Plan
Appendix D. Multi-Entity Group Projects
Appendix E. Imminent Cybersecurity Threats Process Overview
Appendix F. Investment Justification Template and Instructions
Appendix G. Required, Encouraged, and Optional Services, Memberships, and Resources
Appendix H. Economic Hardship Cost Share Waiver

Appendix A: Goals and Objectives

Our nation faces unprecedented cybersecurity risk due to increasingly sophisticated adversaries, widespread vulnerabilities in commonly used software and hardware, and broad dependencies on networked technologies for the delivery of National Critical Functions, the disruption of which would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Cyber risk management is particularly complex due to several factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyber and physical systems, and the difficulty of reducing vulnerabilities in cyber infrastructure. In light of the risk and potential consequences of cyber incidents, strengthening the cybersecurity practices and resilience of SLT governments have become an important homeland security mission.

As part of DHS, CISA is at the heart of mobilizing a collective defense to understand and manage risk to our critical infrastructure partners. In its unique role, CISA is proactively working to achieve a cybersecurity ecosystem in which malicious actors face insurmountably high costs to execute damaging intrusions, vulnerabilities are rapidly identified before exploitation, and technology is used to reduce the most harmful and systemic risks. CISA programs and services are driven by a comprehensive understanding of the risk environment and the corresponding needs identified by our partners. The SLCGP is key to achieving this vision and enables the Department to make targeted investments in SLT government agencies, improving the security and resilience of critical infrastructure upon which Americans rely. The goals and objectives outlined below, if achieved, will significantly reduce the risk of a cybersecurity threat against SLT government information technology (IT) networks.

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

The program goals for the SLCGP are as follows: (1) develop and establish appropriate governance structures, as well as develop, implement, or revise cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations; (2) ensure SLT agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments; (3) implement security protections commensurate with risk (outcomes of Objectives 1 & 2); and (4) ensure organization personnel are appropriately trained in cybersecurity, commensurate with their responsibilities.

These program objectives are further divided into sub-objectives and outcomes, as well as sample evidence of implementation are provided to assist the reader.

Goal of the State and Local Cybersecurity Grant Program: Assist SLT governments with managing and reducing systemic cyber risk.

OBJECTIVE 1: Develop and establish appropriate governance structures, as well as develop, implement, or revise cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.

Sub-objective 1.1: Establish cybersecurity governance structures and implement a program to evaluate maturity of the cybersecurity program aligned to Cybersecurity Performance Goals established by CISA and the National Institute of Standards and Technology (NIST).

1.1.1. *Outcome*: 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.

1.1.2. *Outcome*: Participants have identified senior officials to enable whole-of-organization coordination on cybersecurity policies, processes, and procedures.
- **Sample Evidence of Implementation:** Organization has a cybersecurity defense concept of operations, with responsibilities assigned to specific organizational roles.

Sub-objective 1.2: Develop, implement, or revise, and test cybersecurity plans, including cyber incident response plans, with clearly defined roles and responsibilities.

1.2.1 *Outcome*: Develop, implement, or revise, and exercise cyber incident response plans.
- **Sample Evidence of Implementation:** Organization conducts annual table-top and full-scope exercises that include practical execution of restoration and recovery processes to test cybersecurity plans. Conducting these exercises allow organizations to test cybersecurity plans to identify, protect, detect, respond to, and recover from cybersecurity incidents, in line with the NIST Cybersecurity Framework, and demonstrates process to incorporate lessons learned from the exercise into their cybersecurity program.

Sub-objective 1.3: Asset (e.g., devices, data, software) protections and recovery actions are prioritized based on the asset's criticality and business value.

1.3.1 *Outcome*: Ensure that systems and network functions are prioritized and reconstituted according to their impact to essential functions.
- **Sample Evidence of Implementation:** Organization conducts a regular business impact assessment to prioritize which systems must be protected and recovered first.

OBJECTIVE 2: SLT agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.

Sub-objective 2.1: Physical devices and systems, as well software platforms and applications, are inventoried.

2.1.1 *Outcome*: Establish and regularly update asset inventory.
- **Sample Evidence of Implementation:** Organization maintains and regularly updates an asset inventory list.

Sub-objective 2.2: Cybersecurity risk to the organization's operations and assets are understood.

2.2.1 *Outcome*: Conduct an annual cyber risk assessment to identify cyber risk management gaps and areas for improvement

- **Sample Evidence of Implementation:** Organization annually completes the Nationwide Cybersecurity Review (NCSR).

Sub-objective 2.3: Vulnerability scans are performed, and a risk-based vulnerability management plan is developed and implemented.

2.3.1 *Outcome*: Participate in CISA's Vulnerability Scanning service, part of the Cyber Hygiene program.

- **Sample Evidence of Implementation:** Organization is an active participant in CISA's Cyber Hygiene program.

2.3.2 *Outcome*: Effectively manage vulnerabilities by prioritizing mitigation of high impact vulnerabilities and those most likely to be exploited.

- **Sample Evidence of Implementation:** Organization has a plan to manage vulnerabilities based on those with the highest criticality, internet-facing vulnerabilities, as well as known exploited vulnerabilities identified in CISA's Known Exploited Vulnerabilities Catalog.

Sub-objective 2.4: Capabilities are in place to monitor assets to identify cybersecurity events.

2.4.1 *Outcome*: SLT 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.

Sub-objective 2.5: Processes are in place to action insights derived from deployed capabilities.

2.5.1 *Outcome*: SLT agencies are able to respond to identified events and incidents, document root cause, and share information with partners.

OBJECTIVE 3: Implement security protections commensurate with risk (outcomes of Objectives 1 & 2)

Sub-objective 3.1: SLT agencies adopt fundamental cybersecurity best practices.

3.1.1 *Outcome*: Implement multi-factor authentication (MFA), prioritizing privileged users, Internet-facing systems, and cloud accounts.

- **Sample Evidence of Implementation:** The organization implements MFA for all remote access and privileged accounts.

3.1.2. *Outcome*: End use of unsupported/end of life software and hardware that are accessible from the Internet.

- **Sample Evidence of Implementation:** The organization has a program to anticipate and discontinue use of end of life software and hardware.

3.1.3 *Outcome*: Prohibit use of known/fixed/default passwords and credentials.

- **Sample Evidence of Implementation:** The organization has a policy that prohibits fixed passwords, requires known/default passwords be immediately changed, and that passwords and credentials be periodically changed.
- **Sample Evidence of Implementation:** The organization has reviewed all of its current passwords and credentials to ensure they are updated appropriately.

3.1.4 *Outcome*: Ensure the ability to reconstitute systems following an incident with minimal disruption to services.

- **Sample Evidence of Implementation:** Organization policies require that backups for all critical systems and data be maintained, updated, and regularly tested according to organizational policy (e.g., quarterly), stored offline, and encrypted.

3.1.5 *Outcome*: Migrate to .gov internet domain.

- **Sample Evidence of Implementation:** Organization operates only the .gov internet domain, and does not use .com, .org, or any other domain.

Sub-Objective 3.2: Reduce gaps identified through assessment and planning process and apply increasingly sophisticated security protections commensurate with risk.

3.2.1 *Outcome*: Individual participants address items identified through assessments and planning process.

3.2.2 *Outcome*: SLT entities improve cybersecurity ecosystem by collaborating to address items identified through assessments and planning process (e.g., regional and intra-state efforts)

Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Sub-Objective 4.1: Train personnel to have the fundamental knowledge and skills necessary to recognize cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices.

4.1.1 *Outcome*: Organization requires regular ongoing phishing training, awareness campaigns are conducted, and organization provides role-based cybersecurity awareness training to all employees.

4.1.2 *Outcome*: Organization has dedicated resources and funding available for its cybersecurity professionals to attend technical trainings and conferences.

Sub-Objective 4.2: Organization has adopted the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

4.2.1 *Outcome*: Organization has established cyber workforce development & training plans, based on the NICE Cybersecurity Workforce Framework.

Appendix B: Planning Committee

Governance

In keeping with the guiding principles of governance for all Federal Emergency Management Agency (FEMA) preparedness programs and statutory requirements, recipients must coordinate activities across preparedness disciplines and levels of government, including SLT governments. A cohesive planning framework should incorporate FEMA resources, as well as those from other federal and SLT entities, the private sector, and faith-based community organizations. Specific attention should be paid to how available preparedness funding sources can effectively support a Whole Community approach to emergency preparedness and management and the enhancement of Core Capabilities. To ensure this, the State Administrative Agency (SAA) must establish or reestablish a unified Cybersecurity Planning Committee. A Cybersecurity Planning Committee is also required pursuant to the statute authorizing the SLCGP (see section 2220A(g) of the Homeland Security Act of 2002, as amended (6 U.S.C. § 665g(g)).

Cybersecurity Planning Committee

The Cybersecurity Planning Committee builds upon previously established advisory bodies under other preparedness grant programs. The membership of the Cybersecurity Planning Committee must reflect an eligible entity's unique cybersecurity risk profile.

An existing multijurisdictional planning committee must meet the membership requirements as outlined in the next section, or the existing committee's membership can be expanded or leveraged to meet the membership requirements as well as the unique requirements of each eligible entity. It is recommended that eligible entities consider using Senior Advisory Committees or create a subcommittee within an existing multijurisdictional committee for this purpose, modified to meet the membership and purpose requirements. Any reference to a Cybersecurity Planning Committee elsewhere in this NOFO, and the accompanying requirements, also apply to these alternative planning committee options.

Cybersecurity Planning Committee Composition and Scope Requirements

Cybersecurity Planning Committee membership shall include at least one representative from relevant stakeholders including:

- The eligible entity;
- The Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or equivalent official of the eligible entity;
- If the eligible entity is a state (including territories), then representatives from counties, cities, and towns within the jurisdiction of the eligible entity;
- Institutions of public education and health within the jurisdiction of the eligible entity; and
- As appropriate, representatives of rural, suburban, and high-population jurisdictions.

At least one half of the representatives of the Cybersecurity Planning Committee must have professional experience relating to cybersecurity or information technology. Qualifications are determined by the states.

Eligible entities are given the flexibility to identify the specific public health and public education agencies and communities these members represent.
DHS strongly encourages eligible entities to consider naming additional members to the Cybersecurity Planning Committee, including but not limited to representatives from:

- State and county judicial entities;
- The Chief Information Officer (CIO), the Chief Information Security Officer (CISO, or equivalent official of the eligible entity;
- State legislature;
- Election Infrastructure officials, including Secretaries of State and Election Directors;
- Representatives from state, territorial, and local public safety, homeland security, emergency management, and law enforcement agencies;
- Emergency Communications Officials, such as Interoperability Coordinators;
- City and county CIOs and CISOs;
- Publicly owned or operated critical infrastructure;
- State National Guard if such entities have a cybersecurity mission;
- Municipal, city, county, rural area, or other local government councils or associations; and
- Other entities with expertise and skillsets that best represent the cybersecurity interests across the eligible entity.

The composition, structure, and charter of the Cybersecurity Planning Committee should focus on building cybersecurity capabilities across the eligible entity instead of simply combining previously existing advisory bodies under other grant programs. The Cybersecurity Planning Committee POC's contact information must be provided to FEMA as part of the grant application. Eligible entities must ensure that information for current points of contact is on file with FEMA.

Eligible entities must submit the list of Cybersecurity Planning Committee members at the time of application as an attachment in ND Grants. Eligible entities must verify compliance with Cybersecurity Planning Committee charter requirements. The below table provides a suggested format for submitting the list of required Cybersecurity Planning Committee members.

Planning Committee Membership				
Representation	**Name**	**Title**	**Organization**	**Cybersecurity/IT Experience (Yes/No)**
Eligible entity				
If eligible entity is a state, counties, cities, and towns within the jurisdiction of the entity				

Institution of Public Education within the eligible entity				
Institution of Public Health within the eligible entity				
(Additional)				
As appropriate, representatives of rural, suburban, and high-population jurisdictions				
(here the entity may add others at their discretion)				

Cybersecurity Planning Committee Responsibilities
The responsibilities of the Cybersecurity Planning Committee include:

- Assisting with the development, implementation, and revision of the Cybersecurity Plan;
- Approving the Cybersecurity Plan;
- Assisting with the determination of effective funding priorities;
- Coordinating with other committees and like entities with the goal of maximizing coordination and reducing duplication of effort;
- Creating a cohesive planning network that builds and implements cybersecurity preparedness initiatives using FEMA resources, as well as other federal, SLT, private sector, and faith-based community resources;
- Ensuring investments support closing capability gaps or sustaining capabilities; and
- Ensuring local government members, including representatives from counties, cities, and towns within the eligible entity provide consent on behalf of all local entities across the eligible entity for services, capabilities, or activities provided by the eligible entity through this program.

Limitations
Cybersecurity Planning Committees that meet the requirements of this NOFO and the statute are not permitted to make decisions relating to information systems owned or operated by, or on behalf of, the state.

Local Consent
Eligible entities or multi-entity groups are statutorily required to provide at least 80% of the federal funding to local governments, including at least 25% rural areas. With the consent of the local governments, part or all of this pass-through can be in the form of items, services, capabilities, or activities. This flexibility in the type of funds that are passed through may assist eligible entities or multi-entity groups in promoting projects that have state-wide (or broader)

impacts, and they may be able to more effectively reduce cybersecurity risk if managed at the state or multi-state level. Examples of these types of projects include the purchase of software licenses or development of capabilities. Any decision to pass through some or all of the funds via items, services, capabilities, or activities must be explicitly consented to by the local governments and must be documented in accordance with the Cybersecurity Planning Committee's Charter and comply with Section F.2 of this NOFO for further information.

Cybersecurity Planning Committee Charter
The governance of the SLCGP through the Cybersecurity Planning Committee should be directed by a charter. All members of the Cybersecurity Planning Committee should sign and date the charter showing their agreement with its content and their representation on the committee. Eligible entities must submit the Cybersecurity Planning Committee charter at the time of application as an attachment in ND Grants. Revisions to the governing charter must also be sent to the recipient's assigned FEMA HQ Preparedness Officer. The Cybersecurity Planning Committee charter must, at a minimum, provide:

- A detailed description of the Cybersecurity Planning Committee's composition and an explanation of key governance processes;
- A description of the frequency at which the Cybersecurity Planning Committee will meet;
- An explanation as to how the committee will leverage existing governance bodies;
- A detailed description of how decisions on programmatic priorities funded by SLCGP will be made and how those decisions will be documented and shared with its members and other stakeholders, as appropriate; and
- A description of defined roles and responsibilities for financial decision making and meeting administrative requirements.

To ensure ongoing coordination efforts, eligible entities are encouraged to share community preparedness information from other preparedness grant programs as submitted in a state's Biannual Strategy Implementation Report with members of the Cybersecurity Planning Committee. Eligible entities are also encouraged to share their Threat and Hazard Identification and Risk Assessment/Stakeholder Preparedness Review data with members of the Cybersecurity Planning Committee who are applying for other FEMA preparedness grants to enhance their understanding of statewide capability gaps.

To manage this effort and to further reinforce collaboration and coordination across the stakeholder community, a portion of the 20% funding holdback of a state (including territories) award may be utilized by the eligible entity to support the Cybersecurity Planning Committee and to ensure representation and active participation of Cybersecurity Planning Committee members. Funding may be used for hiring and training planners, establishing and maintaining a program management structure, identifying and managing projects, conducting research necessary to inform the planning process, and developing plans that bridge mechanisms, documents, protocols, and procedures.

Appendix C: Cybersecurity Plan

Submission of a Cybersecurity Plan is required for any eligible entity participating in the State and Local Cybersecurity Grant Program (SLCGP). The Cybersecurity Plan is a key component of a strategic approach to building cyber resilience. The Cybersecurity Planning Committee, with a holistic membership representing the various stakeholder groups across the entity, is responsible for developing, approving, revising, and implementing the Cybersecurity Plan.

Accordingly, the Cybersecurity Plan should establish high level goals and finite objectives to reduce specific cybersecurity risks at SLT governments across the eligible entity. The Cybersecurity Plan should also serve as the overarching framework for the achievement of the SLCGP goal, with grant-funded projects working to achieve outcomes. Regional approaches, as part of an entity-wide approach, should also be considered.

Cybersecurity Plan Basics

- Comprehensive strategic plan to reduce cybersecurity risk and increase capability across the entity
- Entity-wide plan, not a single entity
- Should cover 2 to 3 years
- Must include required elements, with discretion to add other elements as necessary
- Existing plans can be utilized
- There is no required template, but required elements must be identifiable for review purpose
- Individual projects must align to Cybersecurity Plan
- Must be approved by the Cybersecurity Committee **and** CIO/CISO/Equivalent
- CISA approves for DHS
- Plans are initially approved for 2 years; annually thereafter

In developing the Cybersecurity Plan, the Cybersecurity Planning Committee should consider the following:

- Existing governance and planning documents and identification of any planning gaps that should be addressed by the Cybersecurity Plan;
- Existing assessments and evaluations (e.g., reports, after action reports) conducted by SLT governments within the entity and any planning gaps that require additional assessments and/or evaluations; and
- Identification of potential SLCGP projects to address planning gaps and prioritize mitigation efforts.

Cybersecurity Plan Overview

The following identifies the overall plan requirements and additional considerations that eligible entities should consider when constructing the Cybersecurity Plan. Although there is no required format for the Cybersecurity Plan, Cybersecurity Planning Committees are encouraged to review the Cybersecurity Plan Template, which includes additional details, samples, and templates.

Plan Components

- Roles and responsibilities
- Required elements
- Discretionary elements
- Capabilities assessment
- Implementation plan
- A summary of projects
- Metrics

Cybersecurity Plans must include and address the following items:

- **Incorporate, to the extent practicable, any existing plans to protect against cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, SLTs.** Building upon and incorporating existing structures and capabilities allows entities to provide governance and a framework to meet the critical cybersecurity needs across the entity while making the best use of available resources. For example, consider referencing an existing emergency management plan to address potential downstream impacts affecting health and safety when responding to or recovering from a cybersecurity incident.
- **Describe how input and feedback from local governments and associations of local governments was incorporated.** For states, the SLCGP is intended to reduce cybersecurity risk across the eligible entity. Incorporating input from local entities is critical to building a holistic Cybersecurity Plan.
- **Include the specific required elements** (see Required Elements section of this Appendix below). There are 16 required elements that are central to the Cybersecurity Plan and represent a broad range of cybersecurity capabilities and activities. They also include specific cybersecurity best practices that, when implemented over time, will substantially reduce cybersecurity risk and cybersecurity threats. While each of the 16 required elements must be addressed in the plan, this may include a brief explanation as to why certain elements are not currently being prioritized. Not all 16 elements are required to be aligned to projects and have associated funding. These determinations should be addressed in accordance with capability gaps and vulnerabilities identified through an objective assessment process.
- **Describe, as appropriate and to the extent practicable, the individual responsibilities of the state and local governments within the state in implementing the Cybersecurity Plan.** Defining the roles and responsibilities of SLT governments is critical from both governance and implementation perspectives.
- **Assess the required elements from an entity-wide perspective.** The candid assessment of the current capabilities of SLT entities is the first step in reducing cybersecurity risk across the entity. This assessment also serves as the justification for individual projects. Additional information on the assessment is provided below and in the Cybersecurity Plan Template.
- **Outline, to the extent practicable, the necessary resources and a timeline for implementing the plan.** The Cybersecurity Plan is a strategic planning tool that looks two to three years into the future. Accordingly, it should map how the Cybersecurity Planning Committee seeks to achieve plan goals and objectives. Cybersecurity Plans should address how SLCGP funds will help develop and/or implement the plan. It should also map how other activities and funding sources contribute to the achieving the outcomes described in the plans.
- **Summary of associated projects.** Individual projects are the way elements of the plan are implemented over time. The plan must include a summary of projects associated with each required and discretionary element, designating which will use SLCGP funds. Details for each project using SLCGP funds must be included in the Investment Justification.
- **Describe the metrics that the eligible entity will use to measure progress.** The metrics that will be used must measure implementation of the Cybersecurity Plan and, more broadly, cybersecurity risks reduction across the state. These are different than the

metrics that will be used to measure outcomes of the SLCGP, as described in Section A.10-A.11 and Appendix A of this NOFO. Additional information is provided in the Cybersecurity Plan Metric Section below and also in the Cybersecurity Plan Template.
- **Approvals - the Cybersecurity Plan must be approved by the Cybersecurity Planning Committee and the CIO/CISO/Equivalent.** The eligible entity, upon submitting the Cybersecurity Plan, must certify that the Cybersecurity Plan has been formally approved by the Cybersecurity Planning Committee and the CIO/CISO/Equivalent of the eligible entity.

Cybersecurity Planning Committees should also consider the following when constructing the Cybersecurity Plan:

- **Holistic approach to the Cybersecurity Plan**. The Cybersecurity Plan should be strategic in nature, guiding development of capabilities to address cybersecurity risks and threats across the state or territory. Individual projects should demonstrably support the state, territorial, and local entities in achieving those capabilities over time.
- **Focused investments that are sustainable over time**. The SLCGP currently is authorized for four years and limited funds are available. Cybersecurity Plans must address how SLT entities will sustain capabilities once the program ends or funds are no longer available.
- **State role as leader and service provider.** Many states have significant cyber defenses and elect to provide services to local entities to improve capabilities. Where appropriate, states should consider approaches to support state-wide efforts, that may include using funds to provide services to local entities. Multi-entity projects are another way that eligible entities can group together to address cybersecurity risk and build capabilities (See Appendix D for additional information on multi-entity activities).
- **Building from existing efforts.** Cybersecurity Committees should consider describing how cooperative programs developed by groups of local governments are integrated into the entity-wide approach.
- Additional cybersecurity elements prioritized by the Cybersecurity Planning Committee.

Required Elements

If there are any existing plans that meet the required elements, references to them may be used in lieu of incorporating them in their entirety. The Cybersecurity Plan must describe, to the extent practicable, how the state plans to address the below elements. The Cybersecurity Plan is a strategic document, looking broadly across the entire jurisdiction. The description should support the vision, mission and other strategic guidance set by the Cybersecurity Planning Committee.

1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.

2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.

4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed further below.
   The following cybersecurity best practices under required element 5 must be included in each eligible entity's Cybersecurity Plan:
   - Implement multi-factor authentication;
   - Implement enhanced logging;
   - Data encryption for data at rest and in transit;
   - 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 (backups); and
   - Migration to the .gov internet domain.

   Additional best practices that the Cybersecurity Plan can address include:
   - The National Institute of Standards and Technology (NIST) Cybersecurity Framework;
   - NIST's cyber chain supply chain risk management best practices; and
   - Knowledge bases of adversary tools and tactics.

Required Cybersecurity Best Practices: Although these cybersecurity best practices must be addressed in the Cybersecurity Plan, immediate adoption by every SLT entity is not required. Cybersecurity Plans must clearly articulate efforts to implement these cybersecurity best practices across the eligible entity within reasonable timelines. Individual projects that assist SLT entities adopt these best practices should also be prioritized by the Cybersecurity Planning Committee. As there are multiple ways to implement the best practices, this approach provides committees the flexibility to work with SLT entities to design a plan that takes resource constraints, existing programs, and other factors into account.

6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.

7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.

8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

10. 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 within the jurisdiction of the state.

11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.

12. Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).

13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.

14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.

15. Ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas within the state.

16. Distribute funds, items, services, capabilities, or activities to local governments.

Cybersecurity Planning Committees are strongly encouraged to expand their Cybersecurity Plans beyond the required elements. This may include a focus on specific critical infrastructure or emphasis on different types of SLT entities.

Required Capabilities Assessment

Given the Cybersecurity Plan is a strategic document, it should not identify specific vulnerabilities but instead capture the broad level of capability across the jurisdiction. The assessment will become the road map for individual projects and activities using SLCGP funds. **All Investment Justifications must reference the capability gaps identified in the assessment.** The Cybersecurity Plan Capabilities Assessment Worksheet (see Cybersecurity Plan

Template) provides an easy way for Cybersecurity Planning Committees to capture this information and can be customized as appropriate.

Summary of Projects

Although the Cybersecurity Plan is a strategic document, it must show how individual projects and activities will implement the plan over time. A summary of projects using FY 2022 SLCGP funds associated with each required and discretionary element provides a helpful snapshot of state- and territory-wide capability and capacity that will be achieved as a result of this funding. Details for each project using SLCGP funds must be included in Investment Justification (see Appendix F) and is to include a description of the purpose of the project and what it will accomplish, and, more specifically, how the project will address an identified gap or need and how it supports one or more of the required elements.

The Cybersecurity Plan Template includes a fillable Project Plan Worksheet, a sample of which is below.

- **Column 1**. Project number assigned by the entity
- **Column 2.** Name the project
- **Column 3.** Brief (e.g., 1-line) Description of the purpose of the project
- **Column 4.** The number of the Required Elements the project addresses
- **Column 5.** Estimated project cost
- **Column 6.** Status of project (future, ongoing, complete)
- **Column 7.** Project priority listing (high, medium, low)
- **Column 8.** Project Type (Plan, Organize, Equip, Train, Exercise)]

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**

Cybersecurity Plan Metrics

Cybersecurity Plans must include language detailing how the state will measure both: 1) how the state will implement the plan; and 2) how the state will reduce cybersecurity risks to, and identify, respond to, and recover from cybersecurity threats to, information systems owned or operated by, or on behalf of, the state or local governments within the state. These measures should be at the macro level, related to the goals, objectives, and priorities as part of the overarching strategic plan and not associated with individual projects. See page 6 of this NOFO for additional information on required metrics and reporting.

States, and their Cybersecurity Planning Committees in helping with Cybersecurity Plans, should consider the following when developing metrics:

- Aligning metrics to the Cybersecurity Plan and the established program goals and objectives included at Appendix A.
- Reviewing existing metrics that are in use across the state; and
- The data for each metric must be available and reportable and should not create unnecessary burdens to collect.

The Cybersecurity Plan Template provides a fillable table for reporting metrics.

Sample Table - Cybersecurity Plan Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
1.	1.1		
	1.2		
	1.3		
2.	2.1		
3.	3.1		
	3.2		
4.	4.1		
	4.2		
	4.3		

Appendix D: Multi-Entity Grants

Multiple eligible entities can group together to address cybersecurity risks and cybersecurity threats to information systems within the jurisdictions that comprise the group. There is no separate funding for multi-entity awards. Instead, these investments would be considered as group projects and be funded out of the participating entities' published allocations. These projects should be included as individual Investment Justifications from each participating eligible entity, each approved by the respective Cybersecurity Planning Committee, and each aligned with the eligible entity's Cybersecurity Plan.

Eligibility

In addition to applying as a single entity, an eligible entity (e.g., the SAA) may partner with one or more other eligible entities to form a multi-entity group. Members of multi-entity groups work together to address cybersecurity risks and cybersecurity threats to information systems within their jurisdictions. There is no limit to the number of participating entities in a multi-entity group. Local entities can be included in the project, but their respective eligible entity (i.e., State) must also participate at some level. There is no separate funding for multi-entity awards. Instead, they should be considered as group projects within their existing state or territory allocations. Projects should be included as individual Investment Justifications from each participating eligible entity, each approved by the respective Planning Committee and aligned with each respective eligible entity's Cybersecurity Plan.

Additionally, note that for multi-entity groups, all individual eligible entities must have already developed a Cybersecurity Plan.

Benefits

Cost Savings:

A multi-entity grant will be counted against the total apportionment of each entity. However, multi-entity grants may permit smaller entities to combine resources with larger entities to reap the benefits associated with larger acquisitions. At the same time, all parties to a multi-entity grant may realize cost savings due to volume purchases. The multi-entity group will also benefit from a total of 10% reduction in cost share requirements for that specific project. For FY 2022, this means that multi-entity projects would not require any recipient cost share.

Shared Resources:

Since the multi-entity group may be comprised of state (including territorial) governments, each shall benefit from information sharing and awareness opportunities.

Requirements and Process Overview

- Eligible entities work collaboratively to define the group project and the roles and responsibilities for each eligible entity.
- Each eligible entity must have a Cybersecurity Plan that has been approved by CISA – there is no exception to allow multi-entity groups to use a grant to develop any entity's Cybersecurity Plan.
- The project must improve or sustain capabilities identified in the respective Cybersecurity Plans for each eligible entity.

- The Cybersecurity Planning Committee of each participating eligible entity must approve the individual project.
- Each eligible entity will be required to submit an Investment Justification describing the following:
    - A description of the overarching multi-entity project;
    - The other eligible entities and all participating state, local, tribal, and territorial entities and identify the division of responsibilities amongst the multi-entity group;
    - The distribution of funding from the grant among the eligible entities that comprise the multi-entity group, to include any subawards made to local entities; and
    - How the eligible entities that comprise the multi-entity group will work together to implement the Cybersecurity Plan of each of those eligible entities.

Additional details can be found in Appendix F – Investment Justification.
Note: It is expected that Investment Justifications for multi-entity projects will be almost identical. Any differences should be as a result of alignment with the entities' respective Cybersecurity Plans.

Appendix E: Imminent Cybersecurity Threat

The SLCGP is primarily a security preparedness program focused on reducing cyber risks by helping SLT entities address cybersecurity vulnerabilities and build cybersecurity capabilities. Over time, the program activities and investments will reduce the potential impact of cybersecurity threats and incidents. The State and Local Cybersecurity Improvement Act enumerates, as one eligible use of funds, activities that address imminent cybersecurity threats, as follows: "An eligible entity that receives a grant under this section and a local government that receives funds from a grant under this section, as appropriate shall use the grant to…(4) assist with activities that address imminent cybersecurity threats as confirmed by the Secretary, acting through the [CISA] Director, to the information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity." 6 U.S.C. § 665g(d)(4).

The following provides an overview of the processes for the FY 2022 grant cycle from a grant management perspective. Specific details on CISA's criteria and process for confirming an imminent cybersecurity threat are not included here. The following also does not supersede or replace existing threat notification procedures or existing methods to collaborate on operational cybersecurity matters.

Process Overview

- Any eligible entity seeking to use SLCGP funds to address an imminent cybersecurity threat, as confirmed by the Secretary, acting through the CISA Director, must have a Cybersecurity Plan approved by CISA unless DHS has granted the eligible entity an exception for the FY 2022 grant cycle to use the grant to develop a Cybersecurity Plan.
- Only DHS, through CISA, confirms an imminent cybersecurity threat.
- SLT entities cannot request a threat to be confirmed an imminent cybersecurity threat.
- Upon confirmation, DHS will notify the State Administrative Agency (SAA) at the eligible entity. DHS will notify impacted SLT entities as appropriate.
- FEMA will issue an Information Bulletin detailing the impacted entities and procedures for reprograming SLCGP funds in support of the specific imminent cybersecurity threat. The scope of the Information Bulletin will be dependent on the nature of the imminent cybersecurity threat.
- The eligible entity must notify the Cybersecurity Planning Committee and chief information officer (CIO)/chief information security officer (CISO)/equivalent of the eligible entities, which are responsible for reviewing, prioritizing, and approving projects under SLCGP.
    - Impacted SLT entities should be notified consistent with established governance structures and notification processes within the eligible entity.
- It will be left at the discretion of eligible entity, in consultation with the Cybersecurity Planning Committee and CIO/CISO/equivalent, and in collaboration with other entities as necessary, to review the imminent cybersecurity threat information and determine if SLCGP funds are to be used to assist with activities that address the imminent cybersecurity threats.
- If the eligible entity wants to use any of its grant funds to address imminent cybersecurity threats that may arise during the period of performance, the eligible entity must include

this in and submit an Investment Justification aligned to Objective 3. There is no minimum amount that the eligible entity must request or reserve through this Investment Justification, and if the eligible entity needs to reallocate funding across its approved Investment Justifications to address imminent cybersecurity threats, the eligible entity should collaborate with any subrecipient potentially impacted by the reallocation of funds.

Appendix F: Investment Justification Form and Instructions

Overview

Only one application will be submitted by the eligible entity. The application will consist of up to four (4) Investments, one for each SLCGP objective (see Appendix A for more information on the goal and objectives).

Investments for SLCGP Objectives 1, 2, and 3 must have at least one project. Investments for SLCGP Objective 4 are optional for the FY 2022 SLCGP. If an IJ is submitted for Objective 4, then it also must have at least one project.

For each objective, whether required or optional, Applicants must submit up to one IJ form per SLCGP objective, and at least one Project Worksheet for each submitted Investment Justification. Each IJ should have the same application-level information. Project level information should vary based on the associated SLCGP Objective.

Use the following naming convention for the IJs and Project Worksheets: [Insert name of state or territory] Objective [insert number of corresponding objective – 1, 2, 3 or 4]. For example: Alaska Objective 2.

Multi-entity efforts must be included as individual projects in the Project Worksheet, aligned to the appropriate investment (i.e., SLCGP objective). Additional information is provided below

General Process

- Download IJ Template
- Download IJ Project Worksheet
- Save a separate IJ Template and Project worksheet for each SLCGP Objective.
- Add the same portfolio information to each IJ file.
- Complete the investment level information for each objective.
- Identify individual projects for each objective using the Project Worksheet.
- Submit the following files via ND Grants:
    - Cybersecurity Plan (unless requesting an exemption)
    - One (1) IJ form for each SLCGP objective.
    - One (1) Project worksheet for each SLCGP objective.

The IJ Template and special completion instructions are provided below as a reference, but applicants should download the IJ Template at the link provided above to complete for each SLCGP objective. The IJ Template used for this program is from the approved collection for the Homeland Security Grant Program, but many of the elements still apply to SLCGP. The instructions in the last column explain how a field in the IJ Template applies or does not apply to SLCGP. Please contact the applicable FEMA Preparedness Officer if unsure whether any elements of the IJ Template are required to be filled out.

Paperwork Burden Disclosure Notice:

Public reporting burden for this data collection is estimated to average 72 hours per response. The burden estimate includes the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and submitting this form. This collection of information is required to obtain or retain benefits. You are not required to respond to this collection of information unless a valid OMB control number is displayed on this form. Send comments regarding the accuracy of the burden estimate and any suggestions for reducing the burden to: Information Collections Management, Department of Homeland Security, Federal Emergency Management Agency, 500 C Street, SW., Washington, DC 20472-3100, Paperwork Reduction Project (1660-0125) NOTE: Do not send your completed form to this address.

HSGP IJ PLANNING TEMPLATE	SLCGP SPECIAL INSTRUCTIONS
The IJ Template is useful for the Portfolio and Investment section questions. For the project section, applicants should use the Project Worksheet to record all proposed projects. The Project Worksheet is available at grants.gov. The template allows applicants to use spelling and grammar as well as character count functions available in MS Word during the IJ development process. To ensure adherence with formatting requirements, applicants are strongly encouraged to utilize these functions prior to copying text from MS Word to the Grant Reporting Tool (GRT). Please note that character count limits include spacing and all forms of punctuation. To simplify the transfer of the narrative information section into the GRT, it is also recommended that applicants save a working copy of this Template, deleting Part III and the Appendix.	The GRT will NOT be used for the SLCGP. Instead, applicants must use the MS Excel version of the Project Worksheet and submit one file for each SLCGP Objective.
PART I. PORTFOLIO INFORMATION	
The portfolio provides the overall context for the investments and projects included in the application. The applicant must answer the two portfolio questions only once.	*The portfolio provides the overall context for the investments and projects included in the application. The applicant must answer the two portfolio questions only once. The responses should be copied into each of the IJs.*
I. A. Describe how this portfolio of investments and projects addresses gaps and/or sustainment in the Threat and Hazard Identification Risk Assessment (THIRA)/Stakeholder Preparedness Review (SPR).	
Guidance for Completing this Section (2500 character limit): For purposes of the State Homeland Security Program (SHSP) and the Urban Area Security Initiative (UASI), DHS/FEMA requires states, territories, and Urban Areas to prioritize grant funding to support closing capability gaps or sustaining capabilities identified in the THIRA and SPR process (formerly known as the State Preparedness Report). Each IJ must describe how proposed investments will help build or sustain capabilities (SPR step 1) and/or address capability gaps and sustainment needs (SPR step 2) to help them achieve capability targets (THIRA step 3). IJs may also describe how proposed investments will help address functional area gaps identified in the SPR that may not be directly tied to capability targets. At a high level, applicants should identify the relevant portions of their THIRA/SPR that most of the activities in the investment will address. Then applicants must identify how the proposed investment will address one or more of the capability gaps identified in the most recent SPR. The specific capability gap as found in the SPR must be noted in the investment. The applicant should then	A 2500 character limit is allowed for this response. Guidance for Completing this Section: **THIS SECTION IS NOT REQUIRED IF ELIGIBLE ENTITIES IS REQUESTING AN EXEMPTION FROM SUBMITTING A CYBERSECURITY PLAN (SEE NOTICE OF FUNDING OPPORTUNITY PAGE 22 FOR MORE DETAILS ON THE EXEMPTION PROCESS).** If an exemption is being requested, please state "Exemption requested. Section will be updated when Cybersecurity Plan is submitted for review and approval." Applicants will be required to update this section once the Cybersecurity Plan is submitted for review, along with updated individual projects. **THE FOLLOWING ASSESSMENT IS REQUIRED IF AN eligible entity IS SUBMITTING A CYBERSECURITY PLAN FOR REVIEW BY CISA.**

HSGP IJ PLANNING TEMPLATE	SLCGP SPECIAL INSTRUCTIONS
specifically describe why those proposed activities outlined within the investment are a priority for the applicant.	Applicants should briefly describe the capabilities of the SLT agencies across the eligible entity related to the required elements of the Cybersecurity Plan. Note the inclusion of the priority Cybersecurity Best Practices. The description should provide the framework for all investment requests provided within the IJ. It is important to provide the best possible assessment of capabilities of SLT entities within the eligible entity, not only the eligible entity itself. In the case of states, this means including local entities, providing a state-wide assessment of capabilities specifically related to the required elements of the Cybersecurity Plan. Wherever possible, applicants should cite the source (e.g., assessment, survey, exercise) used to evaluate each capability. **Use the list of elements below as headers for each section or subsection, to the extent practicable and as applicable.** 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, and resilience of information systems, applications, and user accounts 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by risk 5. 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. 6. Promote the delivery of safe, recognizable, and trustworthy online services, including through the use of the .gov internet domain 7. Ensure continuity of operations including by conducting exercises 8. 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)

<table>
<tr><th>HSGP IJ PLANNING TEMPLATE</th><th>SLCGP SPECIAL INSTRUCTIONS</th></tr>
<tr><td></td><td>9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks
10. 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
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department
12. Leverage cybersecurity services offered by the Department
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats
15. Ensure rural communities have adequate access to, and participation in plan activities
16. Distribute funds, items, services, capabilities, or activities to local</td></tr>
<tr><td>I. B. Identify the amount and percentage of funding that will be allocated for Management and Administration expenditures.</td><td></td></tr>
<tr><td>Note: The total Management and Administration (M&A) amount and total M&A percentage <u>will not</u> be automatically calculated in the table below. The GRT will automatically calculate the total when applicants transfer their answers. The total M&A percentage may not exceed 5% of the allocated funding. Please note that M&A should be calculated at the portfolio level per funding source (e.g., [State Homeland Security Program (SHSP) or Urban Area Security Initiative (UASI)] and not at the individual Investment level. Any M&A funds retained for the administration of the Operation Stonegarden Program will be reported in the Bi-annual Strategy Implementation Report (BSIR).</td><td>Note: The total Management and Administration (M&A) amount and total M&A percentage <u>will not</u> be automatically calculated in the table below. As the GRT is not being used, applicants will have to calculate the total M&A manually. Please note that M&A should be calculated at the portfolio level – all of SLCGP – and not at the individual Investment level.</td></tr>
</table>

Program	**Requested Amount**	**M&A Amount**	**M&A Percentage**	**Subtotal** (Requested Amount + M&A)
SHSP	$	$	%	$
UASI	$	$	%	$
Total:	**$**	**$**	**%**	**$**

Do not enter any figures here.
Do not enter any figures here.
Enter figures only in the Total row.

HSGP IJ PLANNING TEMPLATE	SLCGP SPECIAL INSTRUCTIONS
PART II. SPECIFIC INVESTMENT INFORMATION	
II. A. Provide the Investment name: (100 character limit)	Insert the related objective (i.e., "Objective 1", "Objective 2", "Objective 3" or "Objective 4"). No additional text is needed.
II. B. Investment Type: Choose one of the following from the GRT dropdown menu: Consolidated Fusion Center Investment, Consolidated Cybersecurity Investment, or Standard Investment	Select "Consolidated Cybersecurity Investment" from the dropdown menu.
Please note that all fusion center-related funding requests **must be consolidated into a single investment per funding source** (e.g., SHSP or UASI) in which recognized fusion centers reside. The consolidated fusion center Investment per funding source must address direct funding support for the recognized fusion center. For a list of recognized fusion centers, please see (http://www.dhs.gov/fusion-center-locations-and-contact-information). Also note that there must be at least one investment in support of the state, urban area or territory's cybersecurity efforts.	N/A
II. C. What is the funding source for this investment: Each investment must identify a programmatic funding source (SHSP or UASI). If a project will use multiple sources of funding, separate the amounts of funding from each source under different investments. If UASI funds are used by the eligible entity in support of the Urban Area, the eligible entity must, as part of the up to 10 UASI investments, propose an investment describing how UASI funds will be used by the eligible entity to directly support the Urban Area.	**N/A**

Funding Source		**Funding Amount**	
Proposed Funding Source (*Select One*)		$	N/A
Proposed Amount		**$**	**Enter total proposed funding for the entire investment (i.e., all projects associated with SLCGP Objective)**

II. D. How much of this Investment will be obligated towards Law Enforcement Terrorism Prevention Activities (LETPA)? $	**How much of this investment will be obligated towards local and rural governments?** **Enter the local total followed by the rural total, using "/" between the two numbers. For example: $100/$50**
Per section 2006 of the *Homeland Security Act of 2002*, as amended, (6 U.S.C. § 607), FEMA is required to ensure that at least 25 percent (25%) of grant funding appropriated for the Homeland Security Grant Program are used for LETPA. FEMA meets this requirement, in part, by requiring all SHSP and UASI recipients to ensure that at least 25% of grant funding appropriated for grants awarded under HSGP's authorizing statute is used for LETPA. The LETPA allocation can be from SHSP, UASI or both. This requirement does not include award funds from OPSG.	LETPA does not apply to SLCGP but all eligible entities that receive an SLCGP grant are required to ensure that at least 80% of grant funding appropriated for the SLCGP are obligated or otherwise made available to local governments. Additionally, at least 25% of grant funding appropriated for the SLCGP must be obligated or otherwise made available to rural governments within the jurisdiction of the eligible entity, consistent with their Cybersecurity Plan.
II. E. Describe the investment, specifically how it addresses gaps and/or sustainment in the Threat and Hazard Identification Risk Assessment (THIRA)/Stakeholder Preparedness Review (SPR).	The purpose of this section is to describe how projects for each investment (e.g., Objective 1) align to the entity's Cybersecurity Plan. It

HSGP IJ PLANNING TEMPLATE	SLCGP SPECIAL INSTRUCTIONS
	also allows the applicant to describe how implementing the plan will be measured (metrics).
Guidance for Completing this Section (2500, character limit): At a high level, applicants should identify the relevant portions of their THIRA/SPR that most of the activities in the investment will address. Then applicants must identify how the proposed investment will address one or more of the capability gaps identified in the most recent SPR. The specific capability gap as found in the SPR must be noted in the investment. The applicant should then specifically describe why those proposed projects outlined within the investment are a priority for the applicant.	Guidance for Completing this Section: The purpose of this section is to describe how projects for each investment (e.g., Objective 1) align to the entity's Cybersecurity Plan. It also allows the applicant to describe how implementing the plan will be measured (metrics). **IF AN EXEMPTION FROM THE CYBERSECURITY PLAN IS REQUESTED IN SECTION I.A. (SEE THE NOTICE OF FUNDING OPPORTUNITY PAGE 22 FOR MORE DETAILS ON THE EXEMPTION PROCESS)** If an exemption is being requested, please state "Exemption requested. Section will be updated when Cybersecurity Plan is submitted for review and approval." Applicants will be required to update this section once the Cybersecurity Plan is submitted for review, along with updated individual projects. **IF AN EXEMPTION FROM THE CYBERSECURITY PLAN IS NOT REQUESTED** **A. Cybersecurity Plan Alignment** • Applicants should list each project and reference the specific sections of their Cybersecurity Plan that each of the projects within this investment are aligned. The applicant should use page numbers and identify specific sections of their Cybersecurity Plan to aid the reviewer in the analysis of the response provided. • Then applicants must identify how the proposed project will address one of the capability gaps referenced in section I.A. The applicant should then specifically describe why those proposed activities outlined within the IJ are a priority for the applicant. **B. Performance Metrics** • Applicants must provide the metrics described in their Cybersecurity Plan. • For each metric, applicants must define key terms, identify the source of the data, how the data is collected, the frequency of data collection, and association to any specific projects, if applicable.
PART III. PROJECT INFORMATION	
All requested funding must be associated with specific projects. For each project, several pieces of information, or attributes, must be provided to submit the project for consideration in the application. The tables below list each attribute, followed by a description and a set of instructions for the applicant to follow to provide the appropriate information.	All requested funding must be associated with specific projects. For each project, several pieces of information, or attributes, must be provided to submit the project for consideration in the application. The tables below

<table>
<tr><th colspan="3">HSGP IJ PLANNING TEMPLATE</th><th>SLCGP SPECIAL INSTRUCTIONS</th></tr>
<tr><td colspan="3">To prepare for completing the IJ in the GRT, applicants should utilize the Project Worksheet (http://www.fema.gov/grants) to plan their applications and to record the necessary information for each project. The Project Worksheet is divided into two tabs: Baseline Project Information and Project Implementation. Once applicants provide a name for a project on the Baseline Project Information tab, the name will auto-populate on the Project Implementation tab.

The Project Worksheet provides drop-down selections for several of the project attributes. The applicant may then use the information collected in the worksheet for rapid transfer to the GRT interface. Each project will be given a unique identifier as it is submitted via the GRT. Applicants should keep a record of the project identifiers as they will be required to report on each project using that identifier.</td><td>list each attribute, followed by a description and a set of instructions for the applicant to follow to provide the appropriate information.

As previously stated, the GRT will not be used, and applicants must submit one Project Worksheet for each SLCGP objective.

The Project Worksheet is divided into two tabs: Baseline Project Information and Project Implementation. Once applicants provide a name for a project on the Baseline Project Information tab, the name will auto-populate on the Project Implementation tab.</td></tr>
<tr><td colspan="3">III. A. Project Alignment to Core Capability Gaps</td><td></td></tr>
<tr><td colspan="3">The first section of project attributes contains basic information about how the projects support or build core capabilities. These attributes are required for every project. If an attribute is left blank in the GRT an error message will appear and the applicant will not be able to submit the application.

The GRT will provide a list of sub-recipients from previous awards. Alternatively, the applicant will have the opportunity to add a new subrecipient to the list. The attribute of `Sub-recipient type' will be auto-populated based on the sub-recipient selection. The applicant must ensure that 80% of the award funds are passed through to local entities.

For additional information on the National Preparedness Goal (NPG) and core capabilities, please visit https://www.fema.gov/national-preparedness-goal.</td><td></td></tr>
<tr><td>Attribute Name</td><td>Description</td><td>Application Instructions</td><td></td></tr>
<tr><td>Project Name</td><td>Descriptive identifier of the project</td><td>Provide a title for specified project (100 character maximum). The title must reflect the nature of work to be completed under the project.</td><td>Provide a title for specified project (100 character max). Title must reflect nature of work to be completed under the project.

Multi-entity projects: Include “multi-entity” at the beginning of the project name.</td></tr>
<tr><td>Project Description</td><td>Descriptive narrative of the project</td><td>Provide a brief narrative describing the project at a high level (1500 character maximum). Identify the National Incident Management System (NIMS) typed resource if any, that is supported by this project. Refer to the Resource Typing Library Tool at http://www.fema.gov/resource-management-mutual-aid.</td><td>Provide a brief narrative describing the project at a high level. (15001500, chars.) NIMS typed resource does not apply.
The first line must identify the required element(s) of the cybersecurity plan the project addresses (see Appendix C of the NOFO). Simply include the number of the required element(s) in brackets separated by a comma. For example: [1,5]. If the project supports the plan development specifically, include [Plan Development].</td></tr>
</table>

HSGP IJ PLANNING TEMPLATE			SLCGP SPECIAL INSTRUCTIONS
			Multi-entity projects: Group project must explicitly include the following in their description: • A description of the overarching multi-entity project; • The other eligible entities and all participating SLT entities and identify the division of responsibilities amongst the multi-entity group; • The distribution of funding from the grant among the eligible entities that comprise the multi-entity group, to include any sub-awards made to local entities; and • How the eligible entities that comprise the multi-entity group will work together to implement the Cybersecurity Plan of each of those eligible entities.
Attribute Name	**Description**	**Application Instructions**	
Recipient Type	State or local recipient for purposes of meeting the 80% pass through requirement	This attribute will auto populate in the GRT based on what state agency or subrecipient is selected.	Input either "State" or "Local".
Project Location	Zip code of the primary location of the project	Provide the 5-digit zip code where the project will be executed. The project location could be distinct from the sub-recipient address.	Provide the 5-digit zip code where the project will be executed. The project location could be distinct from the sub-recipient address.
Primary Core Capability	Primary core capability that the project will impact	Every project must support a core capability. Select the primary core capability associated with this project.	Every project must support a SLCGP Objective. The dropdown box in the Project Worksheet is limited to the Core Capabilities. Use the following options to identify the primary SLCGP objective associated with the project: Objective 1 = Planning Objective 2 = Threats and Hazards Identification Objective 3 = Cybersecurity Objective 4 = Operational Collaboration
Sustain or Build	Indicates whether the project will sustain or build a core capability	Select "build" if this project focuses on starting a new capability or the intent of the project is to close a capability gap (i.e., taking the core capability as a whole from an SPR score 1 to a 2), or "sustain" if the purpose of the project strictly maintains a core capability at its existing current level (i.e., the project does not move the core	Select "build" if this project focuses on starting a new capability or the intent of the project is to close a capability gap or "sustain" if the purpose of the project strictly maintains an existing capability at its existing current level.

HSGP IJ PLANNING TEMPLATE			SLCGP SPECIAL INSTRUCTIONS
		capability as a whole neither up nor down from its existing SPR score).	
Deployable	Indicates if the assets or activities of the project are deployable to other states.	Is the core capability supported by this project deployable to other jurisdictions? (Yes/No)	Select "Yes" the project supports multiple jurisdictions (e.g., multiple cities), entities across the entire eligible entity (e.g., state providing service to local entities), or is a multi-entity project. Select "No" if the project primarily supports a single entity.
Shareable	Indicates if the assets or activities of the project are shareable within the state or with other states because the activities assets are not physically deployable.	Is the core capability supported by this project shareable with other jurisdictions? (Yes/No)	N/A
III. B. Project Alignment to Solution Areas			
The grant funded activities of every project must align to the HSGP solution areas: Planning, Organization, Exercises, Training and/or Equipment (POETE). A project may have activities in more than one solution area. For the POETE funding amounts the GRT will automatically calculate the total amount as you enter funding amounts. For additional information on the allowable cost categories, please refer to the HSGP NOFO.			Complete the following section as originally designed. The grant funded activities of every project must align to the SLCGP solution areas: Planning, Organization, Exercises, Training and/or Equipment (POETE). A project may have activities in more than one solution area. For the POETE funding amounts the Project Worksheet will automatically calculate the total amount as you enter funding amounts.
Attribute Name	**Description**	**Application Instructions**	
Planning	Dollar amount of the project supporting planning	Identify the amount of funds in the project that will be for planning activities.	

HSGP IJ PLANNING TEMPLATE			SLCGP SPECIAL INSTRUCTIONS
Organization	Dollar amount of the project supporting organization	Identify the amount of funds in the project that will be for organization activities.	
Equipment	Dollar amount of the project supporting equipment	Identify the amount of funds in the project that will be for the purchase of equipment.	
Training	Dollar amount of the project supporting training	Identify the amount of funds in the project that will be for training activities.	
Exercises	Dollar amount of the project supporting exercises	Identify the amount of funds in the project that will be for exercise activities.	
Total	Total dollar amount for the project.	Automatically generated by the GRT from the sum of the POETE cost categories.	
II. C. Project Implementation and Management			
For every project, identify the baseline for project implementation according to whether it builds on a previous investment. Not all projects will be linked to previous investments. Next, determine the appropriate project management phase. For new projects, this will likely be the `initiate' or `planning' phase. However, if the project builds on a previous investment, the project may be in a more advanced execution"”" or `control"“" phase. As the project is implemented the recipient will be expected to report on the progress of the project through the management phases. Please reference Appendix A for a detailed description of the Project Management Life-cycle. The applicant will then be required to provide start and end dates for the project, within the36 month period of performance. Finally, indicate whether the activities of the project will require new construction or renovation, retrofitting, or modification of existing structures. This project attribute is required as some project activities may require extensive environmental review which can affect when implementation can begin.			This section does not apply to the SLCGP.
Attribute Name	**Description**	**Application Instructions**	
Does the Project Support a Previously	Indicates whether the project is related to an investment	Select yes if the current project is a continuation of an existing investment that has used grant funds for implementation from previous DHS/FEMA awards.	

HSGP IJ PLANNING TEMPLATE			SLCGP SPECIAL INSTRUCTIONS
Awarded Investment?	awarded in a previous year.		
If yes, from which year?	Fiscal year of the previous award.	If the project is a continuation of a previous investment, select the specific investment from the list.	
If Yes, which investment?	The previously awarded investment that the project supports.	If the project is a continuation of a previous investment, select the specific investment from the list.	
What is the Last Completed milestone of the previous investment?	A description of the last completed milestone from the previously awarded investment.	Please refer to the investment identified above and then identify the last completed milestone from that investment. (250 character maximum)	
Project Management Step	The current Project Life-cycle phase of the previously awarded investment, or the new project.	Select the most applicable step.	
Start Date	Start date of the project/ previously Awarded Investment	Provide the approximate start date of the project, based on the expected notification of an award. If the project is a continuation of a previous investment, provide the approximate start date of that investment.	
End Date	End date of the project/ previously awarded investment	Provide the approximate end date of the project. If the end date is the end of the expected period of performance, provide that.	

HSGP IJ PLANNING TEMPLATE			SLCGP SPECIAL INSTRUCTIONS
Construction Activity	Indicates whether activities of the project will involve construction, renovation, retrofitting or modifications to an existing structure.	Select yes if the project may involve construction related activity.	
APPENDIX A. PROJECT MANAGEMENT LIFE-CYCLE			
The standard definition of a project is a temporary endeavor with a defined beginning and end (usually time-constrained, and often constrained by funding or a deliverable), undertaken to meet unique goals and objectives, typically to bring about beneficial change or added value. Applying this standard to projects using preparedness grant funds, a project is a related set of activities and purchases supporting the building or sustaining of core capabilities; and is associated with a single entity responsible for execution. This approach will allow DHS/FEMA and applicants to categorize the grant funded project as a discrete unit for post-award management, reporting, and monitoring purposes. The main steps and processes of the Project Management Life-cycle are summarized in this table:			
Steps	**Description**	**Process**	
Initiate	The authorization to begin work or resume work on any particular activity.	Involves preparing for, assembling resources and getting work started. May apply to any level, e.g., program, project, phase, activity, task.	
Steps	**Description**	**Process**	
Execute	The period within the project life-cycle during which the actual work of creating the project's deliverables is carried out.	Involves directing, accomplishing, managing, and completing all phases and aspects of work for a given project.	

HSGP IJ PLANNING TEMPLATE			SLCGP SPECIAL INSTRUCTIONS
Control	A mechanism which reacts to the current project status to ensure accomplishment of project objectives. This involves planning, measuring, monitoring, and taking corrective action based on the results of the monitoring.	Involves exercising corrective action as necessary to yield a required outcome consequent upon monitoring performance. Or the process of comparing actual performance with planned performance, analyzing variances, evaluating possible alternatives, and taking appropriate correct action as needed.	
Close Out	The completion of all work on a project. Can also refer to completion of a phase of the project.	Involves formally terminating and concluding all tasks, activities, and component parts of a particular project, or phase of a project.	
For additional information on the Project Management Life-cycle, please visit Project Management Institute's (PMI) *A Guide to the Project Management Body of Knowledge* (PMBOK Guide) at http://www.pmi.org/PMBOK-Guide-and-Standards.aspx. Specifically, applicants are encouraged to reference Chapter three of the PMBOK Guide, *The Standard for Project Management of a Project.*			

Appendix G: Required, Encouraged, and Optional Services, Memberships, and Resources

All SLCGP recipients and subrecipients are required to participate in a limited number of free services by CISA. For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement.

All SLCGP recipients are strongly encouraged to participate in other memberships.

Additional, optional CISA resources are also available in this Appendix

REQUIRED SERVICES AND MEMBERSHIPS

Cyber Hygiene Services

- **Web Application Scanning** is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards.
- **Vulnerability Scanning** evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP.
For more information, visit CISA's Cyber Hygiene Information Page.

Nationwide Cybersecurity Review (NCSR)

The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC.

Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually.

For more information, visit Nationwide Cybersecurity Review (NCSR) (cisecurity.org).

ENCOURAGED SERVICES, MEMBERSHIP, AND RESOURCES

Membership in the Multi-State Information Sharing and Analysis Center (MS-ISAC) and/or Election Infrastructure Information Sharing and Analysis Center (EI-ISAC):

Recipients and subrecipients are strongly encouraged become a member of the MS-ISAC and/or EI-ISAC, as applicable. Membership is free.

The MS-ISAC receives support from and has been designated by DHS as the cybersecurity ISAC for SLT governments. The MS-ISAC provides services and information sharing that significantly enhances SLT governments' ability to prevent, protect against, respond to, and recover from cyberattacks and compromises. DHS maintains operational-level coordination with the MS-

ISAC through the presence of MS-ISAC analysts in CISA Central to coordinate directly with its own 24x7 operations center that connects with SLT government stakeholders on cybersecurity threats and incidents. To register, please visit https://learn.cisecurity.org/ms-isac-registration. For more information, visit MS-ISAC (cisecurity.org).

The EI-ISAC, is a collaborative partnership between the Center for Internet Security (CIS), CISA, and the Election Infrastructure Subsector Government Coordinating Council. The EI-ISAC is funded through DHS grants and offers state and local election officials a suite of elections-focused cyber defense tools, including threat intelligence products, incident response and forensics, threat and vulnerability monitoring, cybersecurity awareness, and training products. To register, please visit https://learn.cisecurity.org/ei-isac-registration. For more information, visit https://www.cisa.gov/election-security.

CISA Recommended Resources, Assessments, and Memberships (not mandatory)

The following list of CISA resources are recommended products, services, and tools provided at no cost to the federal and SLT governments, as well as public and private sector critical infrastructure organizations:

- CYBER RESOURCE HUB
- Ransomware Guide (Sept. 2020)
- Malicious Domain Blocking and Reporting
- Cyber Resilience Review
- External Dependencies Management Assessment
- EDM Downloadable Resources
- Cyber Infrastructure Survey
- Validated Architecture Design Review
- Free Public and Private Sector Cybersecurity Tools and Services

CISA Central: To report a cybersecurity incident, visit https://www.us-cert.gov/report.

For additional CISA services visit the CISA Services Catalog.

For additional information on memberships, visit Information Sharing and Analysis Organization Standards Organization.

Appendix H: Economic Hardship Cost Share Waiver

The Homeland Security Act of 2002, as amended, requires SLCGP recipients in FY 2022 to provide a non-federal cost share of 10% if they are applying as a single entity (6 U.S.C. § 665g(m)(1)). For entities unable to meet the requirement, an economic hardship waiver may be granted by the DHS Secretary (or designee). However, DHS is not able to provide additional funds even if it does grant a cost share waiver. The federal funding will remain at the same amount as indicated by the statutory formula.

Note that there is no cost share requirement for multi-entity groups for FY 2022. In addition, in accordance with 48 U.S.C. § 1469a, the Secretary has issued a blanket waiver of cost share requirements for the insular areas of the U.S. territories of American Samoa, Guam, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands.

Economic Hardship Factors

Requests for cost share waivers may be granted by the Secretary (or designee) to an eligible entity that demonstrates economic hardship.

The statute, at 6 U.S.C. § 665g(m)(2)(C) requires the Secretary (or designee) to consider the following factors when determining economic hardship:

- Changes in rates of unemployment in the jurisdiction from previous years; and
- Changes in the percentage of individuals who are eligible to receive benefits under the supplemental nutrition assistance program established under the Food and Nutrition Act of 2008 (7 U.S.C. § 2011 et seq.) from previous years.

In addition, for FY 2022, the Secretary (or designee) will also consider the following factors in determining economic hardship:

- Demonstration of fiscal distress that could be caused by changes to statewide budgets already approved prior to knowledge of the SLCGP cost share requirement;
- Demonstration that the rate of unemployment has exceeded the annual national average rate of unemployment for three of the past five years;
- Demonstration that the entity has filed for bankruptcy or been placed under third-party financial oversight or receivership within the past three years; and
- For local units of government only, 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.

To be considered for a cost share waiver, eligible entities must meet at least one of the six criteria described above, but do not necessarily need to meet all of them; requests for waivers will be considered on a case-by-case basis and evaluated holistically.

Waiver Request Requirements

Eligible entities that would like to request an economic hardship waiver should submit a waiver request with its FY 2022 SLCGP application submission in ND Grants with the following information in a written narrative:

- The entity’s background/history of economic hardship.

- Any austerity measure(s) the entity has taken to address economic hardship.
- A description of how the lack of a waiver will impact the entity's ability to develop, implement, or revise a Cybersecurity Plan or address imminent cybersecurity threats.
- A detailed justification explaining why the state (or specific local government(s) or specific project(s) if requesting only a partial waiver) is unable to fulfill the cost share requirement. The applicant must identify specific economic hardship(s) and address the factors listed above.

Approval Process

Once a decision on a waiver request is made, the state will be notified in writing. If approved, the award package will indicate that the cost share has been waived in full or in part and might indicate a requirement for the state to submit a revised budget and/or scope (as applicable) for the identified project(s). If the waiver request is approved after the award has been issued, FEMA will amend the award package to indicate the cost share has been waived in full or in part and whether the recipient must submit a revised budget and/or scope (as applicable) for the identified project(s).

Questions regarding the cost share waiver process may be directed to your FEMA Preparedness Officer or the Centralized Scheduling and Information Desk at askcsid@fema.dhs.gov or 1-800-368-6498.