STATE OF NEVADA
MEETING NOTICE AND AGENDA
NEVADA COMMISSION ON HOMELAND SECURITY

Name of Organization: Nevada Commission on Homeland Security
Date and Time of Meeting: Tuesday, March 3, 2020 – 9:00 a.m.

Carson City Location

State Capitol Building
Guinn Room, 2nd Floor
101 N. Carson Street
Carson City, Nevada 89701

Las Vegas Location

Grant Sawyer State Office Building
Governor's Office Conference Room, 5th Floor
555 E. Washington Avenue
Las Vegas, Nevada 89101

Current Voting Membership	
Name	**Title/Organization**
Steve Sisolak	Governor, State of Nevada – Commission Chair
Joseph Lombardo	Sheriff, Las Vegas Metropolitan Police Department – Commission Vice Chair
Darin Balaam	Sheriff, Washoe County Sheriff's Office
Lisa Christensen	Police Officer, Washoe Tribe of Nevada/California
Todd Fasulo	Vice President, Security and Crisis Management, Wynn Resorts
Mitchell Fox	President and Chief Executive Officer, Nevada Broadcasters Association
Frank Gonzales	General (Ret.), Nevada National Guard, State Director, Nevada Selective Service
Ikram Khan, M.D.	President, Quality Care Consultants
Kate Marshall	Lieutenant Governor, State of Nevada
William McDonald	Fire Chief, Las Vegas Fire and Rescue
Charles Moore	Fire Chief, Truckee Meadows Fire Protection District
Richard Perkins	President, The Perkins Company
John Steinbeck	Fire Chief, Clark County Fire Department
Rosemary Vassiliadis	Director of Aviation, Clark County, McCarran International Airport
Patricia Wade	President, Wade Development
Bill Welch	President and Chief Executive Officer, Nevada Hospital Association
Current Non-Voting Membership	
Name	**Title/Organization**
Karen Burke	Federal Security Director, Transportation Safety Administration
Gonzalo Cordova	Protective Security Advisor, Department of Homeland Security Cybersecurity and Infrastructure Security Agency
Christopher Ipsen	(Ret.) Assistant Vice President of Technology, Chief Information Officer, Desert Research Institute
Justin Luna	Chief, Nevada Division of Emergency Management and Homeland Security
William McCurdy II	Assemblyman, Nevada Assembly
Shaun Rahmeyer	Administrator, Nevada Office of Cyber Defense Coordination
Aaron Rouse	Special Agent in Charge, Nevada, Federal Bureau of Investigation

Name of Organization: Nevada Commission on Homeland Security
Date and Time of Meeting: Tuesday, March 3, 2020 – 9:00 a.m.

This meeting will be video or teleconferenced between the locations specified above beginning at 9:00 a.m. The Nevada Commission on Homeland Security (Commission) may take action on items marked "For Possible Action." Items may be taken out of the order presented on the agenda at the discretion of the Chair. Items may be combined for consideration by the Commission at the discretion of the Chair. Items may be pulled or removed from the agenda at any time.

Please Note: Witnesses wishing to have their complete testimony/handouts included in the permanent record of this meeting should provide a written or electronic copy to the Commission administrative support staff. Minutes of the meeting are produced in a summary format and are not verbatim.

1. **Call to Order and Roll Call** – Chair, Governor Steve Sisolak.

2. **Public Comment** – (Discussion Only) – No action may be taken upon a matter raised under this item of the agenda until the matter itself has been specifically included on an agenda as an item upon which action may be taken. Public comments may be limited to three minutes per person at the discretion of the Chair. Comments will not be restricted based on viewpoint.

3. **Approval of Minutes** – (Discussion/For Possible Action) – Chair, Governor Steve Sisolak. The Commission will discuss whether to approve the minutes of the October 21, 2019, Commission meeting.

4. **Update on the Federal Fiscal Year (FFY) 2020 Homeland Security Grant Program (HSGP) Process** – (Discussion Only) – Chief Justin Luna, State Administrative Agent (SAA) and Chief John Steinbeck, Urban Area Administrator (UAA). The Commission will be provided an update on the current status of the FFY 2020 HSGP process to include HSGP timelines, release of the 2020 Notice of Funding Opportunity (NOFO), Metropolitan Statistical Analysis (MSA) rankings, meeting timelines, reporting requirements, and potential deliverables moving forward from the SAA and UAA, Nevada Resilience Advisory Committee, Finance Committee, and the Commission.

5. **Report on the Statewide Adoption of the National Incident Management System** – (Discussion Only) – Chief Justin Luna, Division of Emergency Management and Homeland Security. The Commission will be briefed on the quarterly report on the statewide adoption of, and compliance with, the National Incident Management System, as required by Nevada Revised Statutes (NRS) 239C.310.

6. **Funding of State Resources for Planned Events** – (Discussion Only) – Chair, Governor Steve Sisolak. The Commission will discuss the process and source of funding of State resources for planned events, such as the Nevada National Guard for New Year's Eve support in Clark County.

7. **Public Comment** – (Discussion Only) – No action may be taken upon a matter raised under this item of the agenda until the matter itself has been specifically included on an agenda as an item upon which action may be taken. Public comments may be limited to three minutes per person at the discretion of the Chair. Comments will not be restricted based on viewpoint.

8. **Adjourn** – (Discussion/For Possible Action).

This is a public meeting. In conformance with the Nevada Public Meeting Law, this agenda was posted or caused to be posted on or before 9:00 a.m. on February 27, 2020, at the following locations:

Nevada State Capitol Building, 101 N. Carson Street, Carson City, NV;
Grant Sawyer State Office Building, 555 E. Washington Avenue, Las Vegas, NV;
Nevada State Emergency Operations Center, 2478 Fairview Drive, Carson City, NV;
Clark County Fire Department, 575 E. Flamingo Road, Las Vegas, NV;
Clark County Government Center, 500 S. Grand Central Parkway, Las Vegas, NV; and

Posted to the following websites:

- Nevada Department of Public Safety's Division of Emergency Management and Homeland Security website located at: http://dem.nv.gov/DEM/DEM_Public_Meeting_Information/; and
- Nevada Public Notice Website at: www.notice.nv.gov

We are pleased to make reasonable accommodations for members of the public who are disabled. If special arrangements for the meeting are necessary, or if you need to obtain meeting materials, please notify Karen Hall, Commission support staff, Division of Emergency Management and Homeland Security, 2478 Fairview Drive, Carson City, Nevada 89701 or (775) 687-0300. 24-hour advance notice is requested. Thank you.

DRAFT MEETING MINUTES – For review by the NCHS on 3/3/20

Meeting Minutes
Nevada Commission on Homeland Security

Attendance	**Date**	October 21, 2019	
	Time	9:00 a.m.	
	Carson City Venue	**Legislative Counsel Bureau** Legislative Building – Room 3137 401 S. Carson Street Carson City, NV 89701	
	Las Vegas Venue	**Legislative Counsel Bureau** Grant Sawyer Building – Room 4401 555 E. Washington Avenue Las Vegas, NV 89101	
	Method	Video-Teleconference	
	Recorder	Karen Hall	
Commission Members	**Attendance Status**	**Legislative, Ex-Officio, Nonvoting Members, Staff, and Others**	**Attendance Status**
Governor Steve Sisolak - Chair	X	Karen Burke	X
Joseph Lombardo – Vice Chair	X	Justin Luna	X
Darin Balaam	X	Gonzalo Cordova	Abs
Gregory Cassell	X	Chris Ipsen	Abs
Lisa Christensen	X	William McCurdy II	X
Todd Fasulo	X	Shaun Rahmeyer	X
Mitch Fox	X	Aaron Rouse	X
Frank Gonzales	Abs		
Ikram Khan	X		
Kate Marshall	X	Samantha Ladich - DAG	X
William McDonald	Abs	Karen Hall – DEM/HS	X
Charles Moore	X	Kendall Herzer – DEM/HS	X
Richard Perkins	X	Meagan Werth-Ranson – DEM/HS	X
Rosemary Vassiliadis	X		
Patricia Wade	X		
Bill Welch	X		

1. Call to Order and Roll Call

Governor Sisolak, Chair of the Nevada Commission on Homeland Security (Commission), called the meeting to order. Karen Hall, Nevada Division of Emergency Management and Homeland Security (DEM/HS) performed roll call. Quorum was established for the meeting.

2. Public Comment

Governor Sisolak opened discussion for public comment in all venues. Terry Daus, Information Security Manager, City of Henderson, spoke in support of the Nevada Resilience Advisory Committee (NRAC) recommendation to maintain Cybersecurity as a Strategic Capacity to be Maintained (SCM) in the Federal Fiscal Year (FFY) 2020 Homeland Security Grant Program (HSGP) process. Mr. Daus spoke to his experience as a project manager on multiple HSGP projects to include a template created for business impact analysis that is used statewide, and another pertaining to incident response planning that multiple agencies are still using. Mr. Daus emphasized the importance of HSGP funding for Cybersecurity capability, noting his understanding of 170 cybersecurity attacks against state and local governments since 2013, in addition to 40 attacks against law enforcement agencies. Mr. Daus urged the Commission to understand the importance of maintaining the critical capability of Cybersecurity throughout the state. No other public comment was provided.

3. Approval of Minutes

Governor Sisolak called for a motion to amend or approve the draft minutes as presented from the August 21, 2019, Commission meeting. Dr. Ikram Khan, Quality Care Consultants, motioned to approve the draft minutes as presented. No discussion was presented on the motion. All were in favor with no opposition. Motion passed unanimously.

4. Discussion on the Recommendations of Strategic Capacities to be Maintained for the Federal Fiscal Year (FFY) 2020 Homeland Security Grant Program (HSGP)

Chief Justin Luna, DEM/HS and State Administrative Agent (SAA), and Deputy Chief John Steinbeck, Clark County Fire Department (CCFD) and Urban Area Administrator (UAA), presented the recommendations provided by the Commission's Finance Committee and the NRAC on the strategic capacities to be maintained during the upcoming FFY20 HSGP process.

- Chief Luna spoke to the historical development of the SCM by Deputy Chief Steinbeck and former Chief Caleb Cage, DEM/HS, to come up with a strategic framework to guide allocation decisions for the HSGP in an effort to maintain the most impactful capacities built to date.
- Deputy Chief Steinbeck spoke to the history and strategy of developing the SCM, and the need for a strategy moving forward rather than a year to year effort to build and coordinate different funding sources to maximize and leverage results. The SCM were brought to the Commission last year, and the Commission made some adjustments and approved the SCM to be used in the FFY19 HSGP process. The HSGP process for FFY20 is now approaching, and the building of these capacities and strategy related go far beyond funding capability, but also toward coordination and resource placements. Deputy Chief Steinbeck urged the Commission to focus on the future problem that should there be a gap in funding or limited funds, what areas are considered critical and enough investment has been made that such capacity cannot be left to fall behind.

- Governor Sisolak opened discussion on any questions regarding the information provided so far, and no discussion was presented.
- Chief Luna referred the Commissioners to the historical HSGP funding information provided in the meeting packets, a programmatic narrative report on HSGP projects funded within the past three years, and the inclusion of two sets of recommendations for FFY20 SCM. Chief Luna spoke to the Finance Committee's review of the SCM recommendations provided by the NRAC. That review resulted in the proposed changes noted below:
    - The addition of the Las Vegas Hazardous Materials Team program under the SCM of Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE).
    - The removal of Cybersecurity as a SCM, including the noted programs and core capabilities listed on the document. The reason for removal was presented as many of the cybersecurity projects that have been funded through the HSGP are new and strategically unproven.
    - The addition of the Metropolitan Medical Response System (MMRS) as a program under the SCM of Planning. This addition is to correct an oversight in the past year, as this program should have been included.
- Sheriff Lombardo, Las Vegas Metropolitan Police Department, and Finance Committee Chair indicated that he and Carolyn Levering, City of Las Vegas, had concern that Cybersecurity was included as a SCM. HSGP projects under this category had been poorly managed in previous years with no direction or vision. To approve a substantial amount of money in support of these Cybersecurity projects that could otherwise be allocated to other areas was troublesome. The NRAC recommendations kept cybersecurity as a SCM, and Sheriff Lombardo presented concern that the Finance Committee efforts may be perceived as a rubber stamp of the NRAC recommendation. Sheriff Lombardo indicated his preference to develop a system where the Finance Committee has more influence on the process. If there is a direction given by the Governor, Sheriff Lombardo would like to know what that direction would be, and indicated that he felt the former Cyber Security Committee (CSC) had been successful in addressing this issue, and perhaps that is something that can be revisited.
- Richard Perkins, the Perkins Company, spoke to his conversations with Sheriff Lombardo regarding this matter, but presented concern that Cybersecurity seems to be the number one threat noted in threat assessments year after year. If it is such a threat, rather than stopping efforts to address the capability, perhaps efforts should be refocused on addressing the capability. Dr. Khan agreed with Mr. Perkins, noting efforts placed into that capability in the past and concern on taking away such focus since Cybersecurity is a national threat.
- Lieutenant Governor Kate Marshall inquired if Sheriff Lombardo's concerns were with the financial administration and monitoring of the cyber-specific HSGP grants separate from the fact that Cybersecurity is still seen as a threat to be addressed. Sheriff Lombardo indicated that this was the case, but his concern is the financial piece and not the need for Cybersecurity capability. Individual needs for Cybersecurity capability have been covered under Recovery in the past, but there have been cyber-specific projects that have not used the funding allocated, and those allocations of large amounts of funding is the issue in addition to the lack of individual project direction or oversight. Sheriff Lombardo spoke to a previous

HSGP grant cycle which resulted in the reallocation of over $400,000.00 due to this type of issue. Lieutenant Governor Marshall agreed with the earlier comments made by Mr. Perkins, including that project oversight is crucial for the administration of the grant.

- Governor Sisolak agreed Cybersecurity is an important capacity and inquired if Sheriff Lombardo's suggestion is to still remove Cybersecurity as a SCM. Sheriff Lombardo indicated that his suggestion is still to remove Cybersecurity as a SCM; however, also noting the NRAC chose to leave it as a SCM. The Commission needs to decide which direction to follow. Sheriff Lombardo felt that individual jurisdictions can manage cyber-related capacity as they see fit.
- Governor Sisolak presented concern in allocating resources that were not being used in the program. Deputy Chief Steinbeck indicated that several Cybersecurity projects in the past, except for the two projects Mr. Daus spoke to in public comment earlier, have struggled, and funding had to be returned. This compresses the timeline in being able to effectively reallocate funding. It is never the preference to give funding back to the federal government. Cybersecurity is an extreme threat for Nevada and needs to be addressed, and it is not yet a capacity that is built out such as the fusion centers, bomb squads, hazardous materials teams, or other proven concepts. Should Nevada receive less HSGP funding overall, funding Cybersecurity is a concern. Under the Finance Committee recommendations, Cybersecurity projects would still be eligible for funding competitively. SCM projects have a set allocation that must be proven, and when funded, the balance of funding left goes out for competitive funding. As far as NRAC recommendations go, his understanding is that the NRAC did not recommend returning all the cybersecurity core capabilities back, but rather in the limited capacity of training due to the effectiveness of training efforts to date.
- Dr. Khan inquired on the reasons why the HSGP funding was not utilized for some of the cybersecurity projects in the past. Chief Luna indicated that he did not have specific information on those reasons, and did not wish to speculate; however, he could provide that information later. Cybersecurity has been a requirement in the HSGP guidance for the past several years, and whether the Cybersecurity SCM is included, it is highly likely that the new FFY20 HSGP guidance will more than likely require the inclusion of at least one cyber-specific project.
- Sheriff Darin Balaam, Washoe County Sheriff's Office agreed with Sheriff Lombardo that Cybersecurity projects have struggled in the past, and the individual counties appear to be doing their own cyber-specific programs; however, training is still necessary. In the area of training, this may be where the Cybersecurity capacity has faltered. Training is an area that can be maintained, and reallocating funding has proven difficult as a mechanism to acquire necessary equipment due to timelines associated with the grant performance periods.
- Lieutenant Governor Marshall spoke to concerns on not having the capacity to manage the HSGP grants in this area; specifically, to build the Cybersecurity capacity and create a proper program. By increasing the capacity, the Lieutenant Governor inquired if that action could facilitate the attainment of larger grants from the federal government in the future. States that have built out such capacity might be better positioned to receive such grants. The Lieutenant Governor also spoke to the state's Enterprise Information Technology System (EITS) amending their budget since they have requested historically large projects.

- Shaun Rahmeyer, Office of Cyber Defense Coordination (OCDC), added additional context to the discussion, and offered to assist with answering the question about the grant application assigned to the University of Nevada Reno (UNR) last year. Mr. Rahmeyer agreed with the concern presented regarding Cybersecurity, which is why he, and former Chief Caleb Cage, worked together following the HSGP cycle, the inception of NRAC and OCDC, and the dissolution of the Cyber Security Committee. There were many moving parts, and the responsibility regarding equity in Cybersecurity initiatives is what OCDC has taken on for the state. With the changes that have occurred, there were several decisions that needed to be made to create better mechanisms to allocate funding for Cybersecurity; specifically, aligning efforts towards national frameworks and training as opposed to broad requests. This effort had just begun during the last funding cycle and alleviated the potential lack of funding use. The new process also helps to articulate the Return on Investment (ROI) from these applied funds. A much better picture can now be painted on where funding is applied and utilized. Regarding the funding allocated for UNR, the issue was that UNR was not in compliance with the parameters of the federal guidelines, and for that reason, the funding was returned to the state and reallocated for other use. The Governor inquired on what the specific oversight is for determining such a violation. Chief Luna indicated that DEM/HS uses federal guidelines as an oversight mechanism, and his belief was that UNR did not intend to misuse their funding award. If specific awarded projects do not spend allocations for what could be a number of reasons (project is under budget, funding is not spent, etc.), a deobligation process is in place to reallocate funding and extensions may also be available to assist in expending the maximum amount of grant funding received.
- Sheriff Lombardo asked Mr. Rahmeyer if his position or agency will help to address the Cybersecurity funding issue. Mr. Rahmeyer spoke to his agency's legislative mandate to provide statewide direction in Cybersecurity and the identification of areas pertaining to strategic investment in Cybersecurity. That is why there is equity invested in the funding mechanism. Sheriff Lombardo inquired if the OCDC establishes benchmarks for the SCM. Mr. Rahmeyer emphasized his efforts to create best practice. The Center for Internet Security identifies these areas as critical as does the National Institute for Standards and Technology (NIST). There is an extensive array of tools to improve transparency and articulate better ROI incorporating such practices into a security program.
- Dr. Khan asked if there are any consequences in reallocating funding for future use, with Sheriff Lombardo indicating that in the instance of the UNR case, that issue was addressed properly. The federal government's requirements have been met, and there is not any negativity associated with how the funding has been handled. Sheriff Lombardo spoke to his stated conflict with the NRAC recommendation to retain cybersecurity as a SCM; however, he does not have a problem striking that position now noting the explanation of the OCDC responsibility and oversight.
- Deputy Chief Steinbeck spoke to the NRAC recommendation differences pertaining to only the training piece that was added under the SCM of Cybersecurity. Sheriff Lombardo indicated that he would support the NRAC recommendations, and that this review process is how it should work. When

looking at the previous recommendations of the NRAC, and then the Finance Committee recommendations, the Commission can make a formal decision with input from both bodies.

- Deputy Chief Steinbeck put on record that the NRAC voted to not only support the Las Vegas Hazardous Materials Team, but to also have all urban area CBRNE teams funded in the UASI. Similarly, the MMRS program is also to be funded through UASI.
- Dr. Khan indicated if approval of the current direction of discussion required a motion. Governor Sisolak called for a motion; however, Chief Luna wanted to clarify the SCM amendments:
    - On Page 2 of the NRAC recommendation document, as Deputy Chief Steinbeck mentioned, the addition of the Las Vegas Hazardous Materials Team is to be added as a UASI program under the CBRNE SCM;
    - On Page 3 of the NRAC recommendation document, the addition of training is to be added as a core capability under the Cybersecurity SCM; and
    - On the last page of the NRAC recommendations, MMRS is to be added as a UASI program under the Planning SCM.
- Chief Luna also wanted clarification if DEM/HS would be allowed to make any non-substantive changes to the recommendations once approved. The Lieutenant Governor wanted further clarification on the difference of the NRAC and Finance Committee recommendations, in addition to defining non-substantive changes. Chief Luna indicated non-substantive changes would encompass clerical changes in grammar or formatting only. That was acceptable to the Commission.
- Deputy Chief Steinbeck indicated that the recommendation from NRAC on the SCM as written right now for Cybersecurity was only the training portion, and the rest of the core capabilities listed would be struck should the Commission adopt the NRAC recommendations. The Lieutenant Governor clarified her understanding then that training would be the only choice as a core capability under the SCM of Cybersecurity. Deputy Chief Steinbeck indicated that training has the most proven track record so far. In the future, many more of these core capabilities under Cybersecurity will be maintained as proven capabilities. The Lieutenant Governor asked how the Cybersecurity capacity would be built if efforts are not engaged beyond training. Deputy Chief Steinbeck spoke to the SCM as core needs that far outweigh this recommendation today, and there are many other investments into cybersecurity outside of this process. There are multiple items that need to be addressed beyond strategic capacities and the 32 core capabilities, and they all just do not get priority funding if funding levels drop. The Lieutenant Governor inquired if Deputy Chief Steinbeck's view could, in any way, potentially impact the state's ability to receive federal grant funding moving forward to address the Cybersecurity capacity. Deputy Chief Steinbeck stated that he felt that quite to the contrary, it would be an advantage noting After Action Reports (AAR) and the complete review performed after the 1-October incident. Because of those efforts, the Department of Homeland Security (DHS) has a complete review on how funding supported that incident. Deputy Chief Steinbeck believes Nevada has shown DHS a great track record in expense of grant funding from both the state and urban area funding streams. As Nevada is a good steward

of this process, that effort should increase the ability to gain funding and should not limit competitive submissions through the traditional process annually.

- Shaun Rahmeyer spoke to the value of expenditures outside of Cybersecurity, and while training is important, the other core capabilities under this SCM are still staples in a mature framework. The OCDC is dedicated to engaging statewide efforts particularly in rural locations that do not have significant assets to address cyber threats. This support is crucial for rural areas. While the NRAC did identify training, there is not any reason to not address the other core capability areas.
- Sheriff Lombardo motioned to approve the FFY20 SCM to include the addition of the Las Vegas Hazardous Material Team under the SCM of CBRNE, removing the striking of Cybersecurity adding just the core capability of training, and under the SCM of Planning, adding MMRS. Deputy Chief Steinbeck asked for clarification on Sheriff Lombardo's reference to the Las Vegas Hazardous Materials Team, and whether that means to use the NRAC recommendation to make that program a UASI-only program. Deputy Chief Steinbeck spoke to the NRAC recommendation that the UASI have additional capacities, and the UASI would have the ability to build all CBRNE capacity regionally if that seemed appropriate. Sheriff Lombardo amended his motion to reflect Deputy Chief Steinbeck's explanation.
- Mitch Fox, Nevada Broadcasters Association, asked for clarification on the documents being used to reference the motion presented. Sheriff Lombardo indicated that the motion was to remove the striking of Cybersecurity by the Finance Committee in its recommendation, and to reinstate it with the training core capability. It does not affect the core capabilities. Samantha Ladich, Senior Deputy Attorney General, presented concern that Commissioners understand what exactly they are voting on for this agenda item. Governor Sisolak requested that in the future, documents were labeled to help reference against the agenda. Chief Luna indicated he will ensure that occurs in the future.
- Sheriff Lombardo motioned to approve the NRAC recommendations for SCMs as written. Chief Steinbeck clarified that training is added on in addition to maintaining the rest of the core capabilities under Cybersecurity. Per Sheriff Lombardo, that is the case. All were in favor of the motion with no opposition. Motion passed unanimously.

5. Next Steps in the Federal Fiscal Year (FFY) 2020 Homeland Security Grant Program (HSGP) Process

Chief Justin Luna, DEM/HS, SAA, presented the Commission with the steps to be taken next in the FFY 2020 HSGP process to include updates on federal HSGP timelines and the release of the 2020 Notice of Funding Opportunity (NOFO), Metropolitan Statistical Analysis (MSA) timelines and release of Nevada's 2020 MSA ranking, meeting timelines, reporting requirements, and potential deliverables moving forward from the SAA and UAA, Finance Committee, NRAC, and the Commission. Chief Luna spoke to the information presented as tentative at this time. The determination of the SCM lays the foundation for the process, and the completion of the Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) is expected to be complete by the end of calendar year 2019. Along with these state level assessments, the MSA rankings should be forthcoming soon, which will determine the funding allocations for statewide and urban area use. In January 2020, DEM/HS will be releasing FFY20

HSGP project proposal requirements for those interested stakeholders. Project proposals will be due to DEM/HS in February 2020 and will be reviewed by the NRAC and the Las Vegas Urban Area Working Group (UAWG). Cybersecurity-specific and Communication-specific projects will receive an extra layer of review by OCDC and the Statewide Interoperability Coordinator (SWIC) respectively. It is anticipated that the FFY20 HSGP NOFO will be announced between February and March of 2020. Once the federal funding allocations are determined, the FFY20 HSGP projects may be resubmitted again for review in March 2020 to finalize project proposals. FFY20 HSGP project proposals will be prioritized and sent to the Finance Committee for review. Chief Luna indicated that he could work with Sheriff Lombardo offline on the best process to incorporate the Finance Committee's review of project proposals earlier in the HSGP process. Typically, the Finance Committee will review the HSGP project proposals and make funding recommendations to the Commission. Most likely in April 2020, the final HSGP project recommendations will be given to the Commission, and if approved, will result in the FFY20 HSGP grant application being uploaded to the DHS for review. Upon review at the DHS level, the final award will be released, and the grant awards can be sent to subrecipients. Deputy Chief Steinbeck spoke to the UASI process, noting it follows a similar pattern with results reported up through the NRAC and the Commission as informational only. Governor Sisolak inquired if there were any additional comments, and no additional comments were provided.

6. Public Comment

Governor Sisolak opened public comment in all venues. No public comment was presented in any venue.

7. Adjourn

Governor Sisolak called for a motion to adjourn the meeting. A motion to adjourn was presented by Lieutenant Governor Kate Marshall. All were in favor with no opposition. Meeting adjourned.

The Department of Homeland Security (DHS)
Notice of Funding Opportunity (NOFO)
Fiscal Year (FY) 2020 Homeland Security Grant Program (HSGP)

NOTE: If you are going to apply for this funding opportunity and have not obtained a Data Universal Numbering System (DUNS) number and/or are not currently registered in the System for Award Management (SAM), please take immediate action to obtain a DUNS Number, if applicable, and then to register immediately in SAM. It may take four weeks or more after you submit your SAM registration before your registration is active in SAM, then an additional 24 hours for Grants.gov to recognize your information. Information on obtaining a DUNS number and registering in SAM is available from Grants.gov at: http://www.grants.gov/web/grants/register.html.

A. Program Description

1. Issued By
Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Grant Programs Directorate (GPD)

2. Assistance Listings Number (formerly Catalog of Federal Domestic Assistance Number)
97.067

3. Assistance Listings Title (formerly CFDA Title)
Homeland Security Grant Program

4. Funding Opportunity Title
Homeland Security Grant Program
- State Homeland Security Program
- Urban Area Security Initiative
- Operation Stonegarden

5. Funding Opportunity Number
DHS-20-GPD-067-00-02

6. Authorizing Authority for Program
Section 2002 of the *Homeland Security Act of 2002* (Pub. L. No. 107-296, as amended) (6 U.S.C. § 603)

7. Appropriation Authority for Program
Department of Homeland Security Appropriations Act, 2020 (Pub. L. No. 116-93)

8. Announcement Type
New

9. Program Overview, Objectives, and Priorities

Overview

The Fiscal Year (FY) 2020 Homeland Security Grant Program (HSGP) is one of three grant programs that constitute the Department of Homeland Security (DHS)/Federal Emergency Management Agency's (FEMA's) focus on enhancing the ability of state, local, tribal, and territorial governments, as well as nonprofits, to prevent, protect against, respond to, and recover from terrorist attacks. These grant programs are part of a comprehensive set of measures authorized by Congress and implemented by DHS to help strengthen the Nation's communities against potential terrorist attacks. Among the five basic homeland security missions noted in the DHS Quadrennial Homeland Security Review, HSGP supports the goal to Strengthen National Preparedness and Resilience. In FY 2020, there are three components of HSGP:

1) ***State Homeland Security Program (SHSP):*** SHSP assists state, local, tribal, and territorial efforts to build, sustain, and deliver the capabilities necessary to prevent, prepare for, protect against, and respond to acts of terrorism.
2) ***Urban Area Security Initiative (UASI):*** UASI assists high-threat, high-density Urban Areas efforts to build, sustain, and deliver the capabilities necessary to prevent, prepare for, protect against, and respond to acts of terrorism.
3) ***Operation Stonegarden (OPSG):*** OPSG supports enhanced cooperation and coordination among Customs and Border Protection (CBP), United States Border Patrol (USBP), and federal, state, local, tribal, and territorial law enforcement agencies to improve overall border security. OPSG provides funding to support joint efforts to secure the United States' borders along routes of ingress/egress to and from international borders, to include travel corridors in states bordering Mexico and Canada as well as states and territories with international water borders. State, local, tribal, and territorial (SLTT) law enforcement agencies utilize their inherent law enforcement authorities to support the border security mission and do not receive any additional authority as a result of participation in OPSG.

The 2018-2022 FEMA Strategic Plan creates a shared vision for reducing the risks posed by terrorism and sets an ambitious, yet achievable, path forward to unify and further professionalize emergency management across the country. HSGP supports the goals of Building a Culture of Preparedness and Readying the Nation for Catastrophic Disasters. We invite our stakeholders and partners to also adopt these priorities and join us in building a more prepared and resilient Nation, as preparedness is a shared responsibility and funding should support priorities that are most impactful and demonstrate the greatest return on investment.

Finally, for FY 2020, DHS is focused on the criticality of information sharing and collaboration to building a national culture of preparedness and protecting against terrorism and other emerging threats to our national security. DHS and its homeland security mission were born from the "failures among federal agencies and between the federal agencies and state and local authorities to share critical information related to the threat of terrorism" prior to the September 11, 2001, attacks.[1] The threat profile has changed in the last two decades – we now face continuous cyber threats by sophisticated actors, threats to soft targets and crowded places, threats to our democratic election

[1] Homeland Security Act of 2002: Report Together with Minority and Dissenting Views 222, Select Committee on Homeland Security: 107th Congress, U.S. House of Representatives (2002) (H. Rpt. 107-609).

process and threats from new and emerging technologies. But information sharing and cooperation between state, local, and tribal authorities and federal agencies, including all DHS officials, is just as vital, and perhaps even more vital, today. Therefore, for FY 2020, we have identified four priority areas, tied to some of the most serious threats that DHS would like to see addressed by state and local governments, that recipients will need to address with their HSGP funds. Perhaps most importantly, we will be focused on forging partnerships to strengthen information sharing and collaboration in each of these priority areas and looking for recipients to remove barriers to communication and cooperation with DHS and other federal agencies.

Objectives

The objective of the FY 2020 HSGP is to fund state, local, tribal, and territorial efforts to prevent terrorism and prepare the Nation for threats and hazards that pose the greatest risk to the security of the United States.

Priorities

Given the evolving threat landscape, it is incumbent upon DHS/FEMA to continuously evaluate the national risk profile and set priorities that help ensure appropriate allocation of scarce security dollars. In assessing the national risk profile for FY 2020, four priority areas attract the most concern. And due to the unique threats that the nation faces in 2020, DHS/FEMA has determined that these four priorities should be addressed by allocating specific percentages of HSGP funds to each of these four areas, for a total of 20 percent. The following are the four priority areas for FY 2020, along with the corresponding amount of HSGP funds that each recipient will be required to propose for each priority area in order to obtain a full allocation of HSGP funds:

1) Enhancing cybersecurity (including election security) – 5 percent
2) Enhancing the protection of soft targets/crowded places (including election security) – 5 percent;
3) Enhancing information and intelligence sharing and cooperation with federal agencies, including DHS – 5 percent;
4) Addressing emergent threats (e.g., unmanned aerial systems [UASs], etc.) – 5 percent.

Failure by a recipient to propose investments and projects that align with these four priority areas and spending requirements may result in a recipient receiving a reduced grant award. DHS/FEMA may not award funding in excess of a recipient's minimum allocation threshold[2] to the extent that investments and projects do not align with these four priority areas.

A State or high-risk urban area may allocate the remaining 80 percent to gaps identified through their Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Process.

Likewise, there are several enduring security needs that crosscut the homeland security enterprise, and to which that States should consider allocating funding across core capability gaps and national

[2] The *Homeland Security Act of 2002*, as amended, allocates for each of the 50 States, the District of Columbia, and Puerto Rico 0.35 percent of the total funds appropriated for grants under section 2003 and section 2004 of the *Act*, and 0.08 percent for each of the four territories (American Samoa, Guam, the Northern Mariana Islands, and the U.S. Virgin Islands).

priorities. The following are enduring needs that help recipients implement a comprehensive approach to securing communities:

1) Effective planning;
2) Training and awareness campaigns;
3) Equipment and capital projects; and
4) Exercises.

The table below provides a breakdown of the FY 2020 SHSP and UASI priorities (the focus of OPSG remains unique to border security), showing the core capabilities enhanced and lifelines supported, as well as examples of eligible project types for each area. A detailed description of allowable investments for each project type is included in the Preparedness Grants Manual. DHS/FEMA anticipate that in future years, national priorities will continue to be included and will be updated as the threats evolve and as capability gaps are closed. Applicants are strongly encouraged to begin planning to sustain existing capabilities through other funding mechanisms.

FY 2020 SHSP & UASI Funding Priorities

Priority Areas	Core Capabilities	Lifelines	Example Project Types
National Priorities			
Enhancing Cybersecurity (including election security)	• Cybersecurity • Intelligence and information sharing	• Safety and security	• Cybersecurity risk assessments • Projects that address vulnerabilities identified in cybersecurity risk assessments o Improving cybersecurity of critical infrastructure to meet minimum levels identified by CISA o Cybersecurity training and planning
Enhancing the Protection of Soft Targets/ Crowded Places (including election security)	• Operational coordination • Public information and warning • Intelligence and information sharing • Interdiction and disruption • Screening, search, and detection • Access control and identity verification • Physical protective measures • Risk management for protection programs and activities	• Safety and security	• Operational overtime • Physical security enhancements o Security cameras (CCTV) o Security screening equipment for people and baggage o Lighting o Access controls o Fencing, gates, barriers, etc.
Enhancing information and intelligence sharing and cooperation with federal agencies, including DHS	• Intelligence and information sharing	• Safety and security	• Fusion center operations (Fusion Center project will be required under this investment, no longer as a stand-alone investment) • Information sharing with all DHS components, fusion centers, and other entities designated by DHS

			• Cooperation with DHS officials and other entities designated by DHS in intelligence, threat recognition and analysis • Joint training and planning with DHS officials and other entities designated by DHS
Addressing Emergent Threats, such as Transnational Criminal Organizations and UAS	• Interdiction & disruption • Screening, search and detection • Physical protective measures • Intelligence and information sharing • Planning • Public Information and Warning • Operational Coordination	• Safety and security	• Sharing and leveraging intelligence and information • UAS detection technologies • Enhancing weapons of mass destruction (WMD) and/or improvised explosive device (IED) prevention, detection, response and recovery capabilities o Chemical Biological Radiological Nuclear and Explosive (CBRNE) detection, prevention, response, and recovery equipment
Enduring Needs			
Planning	• Planning • Risk management for protection programs and activities • Risk and disaster resilience assessment • Threats and hazards identification • Operational coordination • Community resilience	• Safety and security	• Development of: o Security Risk Management Plans o Continuity of Operations Plans o Response Plans • Efforts to strengthen governance integration between/among regional partners • Joint training and planning with DHS officials and other entities designated by DHS • Cybersecurity training and planning
Training & Awareness	• Long-term vulnerability reduction • Public information and warning • Operational coordination • Situational assessment • Community resilience	• Safety and security	• Active shooter training • Security training for employees • Public awareness/preparedness campaigns • Joint training and planning with DHS officials and other entities designated by DHS • Cybersecurity training and planning
Equipment & Capital Projects	• Long-term vulnerability reduction • Infrastructure systems • Operational communications • Interdiction and disruption • Screening, search and detection • Access control and identity verification • Physical protective measures	• Safety and security	• Protection of high-risk, high-consequence areas or systems that have been identified through risk assessments • Physical security enhancements o Security cameras (CCTV) o Security screening equipment for people and baggage o Lighting o Access Controls ▪ Fencing, gates, barriers, etc.

Exercises	• Long-term vulnerability reduction • Operational coordination • Operational communications • Community resilience	• Safety and security	• Response exercises

Starting in FY 2020, each SHSP and UASI recipient is required to submit an Investment Justification (IJ) for *each* of the four national priorities identified above. Under the Cybersecurity investment and the Soft Target/Crowded Places investments one project for each of those two investments must be to support enhancing election security. As a reminder, all SHSP- and UASI-funded projects must have a demonstrated nexus to preventing, preparing for, protecting against, and responding to acts of terrorism. However, such projects may simultaneously support enhanced preparedness for disasters unrelated to acts of terrorism.

DHS/FEMA also requires SHSP and UASI recipients (e.g., states, territories, and high-risk urban areas) to complete a THIRA/SPR and prioritize grant funding to support closing capability gaps or sustaining capabilities that address national priorities and/or support enduring needs. Additional information on the THIRA/SPR process, including other National Preparedness System (NPS) tools and resources, can be found at https://www.fema.gov/national-preparedness-system. Detailed information on THIRA/SPR timelines and deadlines can be found in the Preparedness Grants Manual.

FY 2020 OPSG Funding Priorities

Priority Areas	Core Capabilities	Lifelines	Example Project Types
National Priorities			
Enhancing information and intelligence sharing and cooperation with federal agencies, including DHS	• Intelligence and information sharing	• Safety and security	• Participation in the DHS/ICE 287(g) training program • Information sharing with all DHS components, fusion centers, and other entities designated by DHS • Cooperation with DHS officials and other entities designated by DHS in intelligence, threat recognition and analysis • Joint training and planning with DHS officials and other entities designated by DHS
Addressing Emergent Threats, such as Transnational Criminal Organizations	• Interdiction & disruption • Screening, search and detection • Physical protective measures • Intelligence and information sharing	• Safety and security	• Operational overtime for border security operations as directed by the applicable, USBP-approved operations order • Sharing and leveraging intelligence and information

Starting in FY 2020, each OPSG applicant is required to clearly articulate and identify how the Concept of Operations addresses *each* of the two national priorities identified above.

10. Performance Metrics

Performance metrics for this program are as follows:

SHSP and UASI:

- Percentage of funding allocated by the recipient to core capabilities to build or sustain national priorities identified in the section above; and

OPSG:

- Number of contacts that occurred as a result of OPSG deployments
    - Number of arrests that resulted from OPSG contacts
    - Value of drug seizures that resulted from OPSG contacts

B. Federal Award Information

Award Amounts, Important Dates, and Extensions

Available Funding for the HSGP NOFO: $1,120,000,000

HSGP Programs	FY 2020 Allocation
State Homeland Security Program	$415,000,000
Urban Area Security Initiative	$615,000,000
Operation Stonegarden	$90,000,000
Total	**$1,120,000,000**

SHSP Allocations

For FY 2020, DHS/FEMA will award SHSP funds based on risk and the anticipated effectiveness of the proposed use of grant funds upon completion of the application review process. The following table identifies the *targeted* SHSP allocation ranges for each State based on DHS/FEMA's relative risk methodology pursuant to the *Homeland Security Act of 2002*, as amended. States are strongly encouraged to apply for funding at least 15% over the high end of their target allocation range as ineffective applications will not be funded. Final award amounts will be based on DHS/FEMA's evaluation of the effectiveness of proposed investments and projects.

Regardless of the amount of a State's targeted SHSP allocation range, each State must include a separate investment for each of the four national priority areas identified in the Priorities section, above. The funding level in each national priority area investment must equal or exceed the percentage for that respective national priority area, calculated as a percentage of the State's *targeted* SHSP allocation in the table below. For the states that receive a target allocation in excess of the minimum, the percentage is calculated against the high end of the range, as displayed in the table below. DHS/FEMA will make final award determinations based upon a review of the anticipated effectiveness of the State's application as described in Section D, below. Final awards are based on whether the State has proposed investments in each of the four national priority areas in an amount equal to or greater than the percentage for that priority area and based on the effectiveness review.

DHS/FEMA will allocate to each state and territory a minimum allocation under the SHSP using thresholds established in the *Homeland Security Act of 2002*, as amended. The minimum allocation for all 50 States, the District of Columbia, and the Commonwealth of Puerto Rico is 0.35 percent of the total funds appropriated for grants under Section 2003 and Section 2004 of the *Homeland Security Act of 2002*, as amended. The minimum allocation for the four territories (American Samoa, Guam, the Northern Mariana Islands, and the U.S. Virgin Islands) is 0.08 percent of the total funds appropriated for grants under Section 2003 and 2004 of the *Homeland Security Act of 2002*, as amended. THIRA/SPR results do not impact grant allocation or award.

Regardless of the final award amount, a state must invest SHSP funding in each of the four national priority areas in an amount equal to or greater than percentage identified above for each national priority area, as approved by DHS/FEMA.

FY 2020 TARGET SHSP ALLOCATIONS

State/Territory	FY 2020 Allocation	State/Territory	FY 2020 Allocation
New York	$59,174,400 - $73,968,000	Kentucky	$4,287,500
California	$49,608,800 - $62,011,000	Louisiana	$4,287,500
Texas	$15,839,200 - $19,799,000	Maine	$4,287,500
Illinois	$12,085,600 - $15,107,000	Minnesota	$4,287,500
Florida	$8,127,200 - $10,159,000	Mississippi	$4,287,500
Virginia	$7,076,800 - $8,846,000	Missouri	$4,287,500
Georgia	$4,600,000 - $5,750,000	Montana	$4,287,500
Pennsylvania	$7,076,800 - $8,846,000	Nebraska	$4,287,500
Maryland	$6,153,600 - $7,692,000	Nevada	$4,287,500
New Jersey	$6,153,600 - $7,692,000	New Hampshire	$4,287,500
Washington	$5,384,800 - $6,731,000	New Mexico	$4,287,500
Massachusetts	$5,384,800 - $6,731,000	North Dakota	$4,287,500
Ohio	$5,384,800 - $6,731,000	Oklahoma	$4,287,500
North Carolina	$4,423,200 - $5,529,000	Oregon	$4,287,500
District of Columbia	$4,423,200 - $5,529,000	Puerto Rico	$4,287,500
Michigan	$4,423,200 - $5,529,000	Rhode Island	$4,287,500
Alabama	$4,287,500	South Carolina	$4,287,500
Alaska	$4,287,500	South Dakota	$4,287,500
Arizona	$4,287,500	Tennessee	$4,287,500
Arkansas	$4,287,500	Utah	$4,287,500
Colorado	$4,287,500	Vermont	$4,287,500
Connecticut	$4,287,500	West Virginia	$4,287,500
Delaware	$4,287,500	Wisconsin	$4,287,500
Hawaii	$4,287,500	Wyoming	$4,287,500
Idaho	$4,287,500	American Samoa	$1,000,000
Indiana	$4,287,500	Guam	$1,000,000
Iowa	$4,287,500	Northern Mariana	$1,000,000
Kansas	$4,287,500	U.S. Virgin Islands	$1,000,000
			$415,000,000

UASI Allocations

Eligible candidates for the FY 2020 UASI program are identified in the table below. Eligibility has been determined through an analysis of relative risk of terrorism faced by the 100 most populous Metropolitan Statistical Areas (MSAs) in the United States, in accordance with the *Homeland Security Act of 2002*, as amended. Detailed information on MSAs is publicly available from the United States Census Bureau at https://www.census.gov/programs-surveys/metro-micro.html. THIRA/SPR results do not impact grant allocation or award.

For FY 2020, DHS/FEMA will award UASI funds based on risk and the anticipated effectiveness of the proposed use of grant funds upon completion of the application review process. The following table identifies the *targeted* UASI allocations for each high-risk urban area based on DHS/FEMA's relative risk methodology pursuant to the *Homeland Security Act of 2002*, as amended. Applicants are strongly encouraged to apply for funding at least 15% over the high end of their target allocation range as ineffective applications will not be funded. Final award amounts will be based on DHS/FEMA's evaluation of the effectiveness of proposed investments and projects.

In its application, each high-risk urban area, through the State, must include a separate investment for each of the four national priority areas identified in the Priorities section, above. The funding level in each national priority area investment must equal or exceed the percentage for that respective national priority area, calculated as a percentage of the high-risk urban area's *targeted* UASI allocation in the table below. The percentage is calculated against the high end of the range, as displayed in the table below. DHS/FEMA will make final award determinations based upon a review of the anticipated effectiveness of the high-risk urban area's application as described in Section D, below. Final awards are based on whether the State has proposed investments in each of the four national priority areas in an amount equal to or greater than the percentage for that priority area and based on the effectiveness review. Regardless of the final award amount, a high-risk urban area must invest UASI funding in each of the four national priority areas in an amount equal to or greater than percentage identified above for each national priority area, as approved by DHS/FEMA.

FY 2020 TARGET UASI ALLOCATIONS

State/Territory	Funded Urban Area	FY 2020 UASI Allocation
Arizona	Phoenix Area	$4,200,000 - $5,250,000
California	Anaheim/Santa Ana Area	$4,200,000 - $5,250,000
	Bay Area	$30,000,000 - $37,500,000
	Los Angeles/Long Beach Area	$54,400,000 - $68,000,000
	Riverside Area	$2,800,000 - $3,500,000
	Sacramento Area	$2,800,000 - $3,500,000
	San Diego Area	$13,520,000 - $16,900,000
Colorado	Denver Area	$2,800,000 - $3,500,000
District of Columbia	National Capital Region	$41,400,000 - $51,750,000
Florida	Miami/Fort Lauderdale Area	$11,800,000 - $14,750,000
	Orlando Area	$2,800,000 - $3,500,000
	Tampa Area	$2,800,000 - $3,500,000
Georgia	Atlanta Area	$5,000,000 - $6,250,000
Hawaii	Honolulu Area	$2,800,000 - $3,500,000
Illinois	Chicago Area	$54,400,000 - $68,000,000
Louisiana	New Orleans Area	$2,800,000 - $3,500,000
Maryland	Baltimore Area	$3,400,000 - $4,250,000
Massachusetts	Boston Area	$13,520,000 - $16,900,000
Michigan	Detroit Area	$4,200,000 - $5,250,000
Minnesota	Twin Cities Area	$4,200,000 - $5,250,000
Missouri	St. Louis Area	$2,800,000 - $3,500,000
Nevada	Las Vegas Area	$4,200,000 - $5,250,000
New Jersey	Jersey City/Newark Area	$15,240,000 - $19,050,000
New York	New York City Area	$143,000,000 - $178,750,000
Oregon	Portland Area	$2,800,000 - $3,500,000
Pennsylvania	Philadelphia Area	$13,520,000 - $16,900,000
	Pittsburgh Area	$2,800,000 - $3,500,000
Texas	Dallas/Fort Worth/Arlington Area	$13,520,000 - $16,900,000
	Houston Area	$19,680,000 - $24,600,000
	San Antonio Area	$2,800,000 - $3,500,000
Virginia	Hampton Roads Area	$2,800,000 - $3,500,000
Washington	Seattle Area	$5,000,000 - $6,250,000
Total		**$615,000,000**

OPSG Allocations

For FY 2020, DHS/FEMA will award OPSG funds based on risk and the anticipated effectiveness of the proposed use of grant funds upon completion of the application review process. The FY 2020 OPSG risk assessment is designed to identify the risk to border security and to assist with the distribution of funds for the grant program. Funding under OPSG is distributed based on the risk to the security of the border and the effectiveness of the proposed projects. Entities eligible for funding are the state, local, and tribal law enforcement agencies

that are located along the border of the United States. DHS/FEMA will make final award determinations based upon a review of the anticipated effectiveness of the State's application as described in Section D, below. The THIRA/SPR process is not required for OPSG.

For the purposes of OPSG, the risk is defined as the potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence.

Based upon ongoing intelligence analysis and extensive security reviews, DHS/CBP continues to focus the bulk of OPSG funds based upon risk analyses. The risk model used to allocate OPSG funds considers the potential risk that certain threats pose to border security and estimates the relative risk faced by a given area. In evaluating risk, DHS/CBP considers intelligence, situational awareness, criminal trends, and statistical data specific to each of the border sectors, and the potential impacts that these threats pose to the security of the border area. For vulnerability and consequence, DHS/CBP considers the expected impact and consequences of successful border events occurring in specific areas.

Threat and vulnerability are evaluated based on specific operational data from DHS/CBP. Threat components present in each of the sectors are used to determine the overall threat score. These components are terrorism, criminal aliens, drug trafficking organizations, and alien smuggling organizations.

Effectiveness of the proposed investments will be evaluated based on the recipient's investment strategy, budget, collaboration, and past performance.

Period of Performance: 36 months
Extensions to the Period of Performance (PoP) are allowed. For additional information on PoP extensions, refer to the Preparedness Grants Manual.

Projected Period of Performance Start Date: September 1, 2020

Projected Period of Performance End Date: August 31, 2023

Funding Instrument: Grant

C. Eligibility Information

1. Eligible Applicants

The State Administrative Agency (SAA) is the only entity eligible to submit HSGP applications to DHS/FEMA, including those applications submitted on behalf of UASI and OPSG 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 SHSP funds. Tribal governments may not apply directly for HSGP funding; however, funding may be available to tribes under the SHSP and OPSG through the SAA.

2. Eligibility Criteria

Eligible high-risk urban areas for the FY 2020 UASI program have been determined through

an analysis of relative risk of terrorism faced by the 100 most populous Metropolitan Statistical Areas (MSAs) in the United States. Subawards will be made by the SAAs to the designated high-risk urban areas.

In FY 2020, OPSG eligible subrecipients are local units of government at the county level or equivalent level of government and Federally recognized tribal governments in states bordering Canada or Mexico and states and territories with international water borders. All applicants must have active ongoing USBP operations coordinated through a CBP sector office to be eligible for OPSG funding.

In FY 2020, OPSG subrecipients eligible to apply for and receive a subaward directly from the SAAs are divided into three Tiers. Tier 1 entities are local units of government at the county level or equivalent and Federally recognized tribal governments that are on a physical border in states bordering Canada, states bordering Mexico, and states and territories with international water borders. Tier 2 eligible subrecipients are those not located on the physical border or international water but are contiguous to a Tier 1 county. Tier 3 eligible subrecipients are those not located on the physical border or international water but are contiguous to a Tier 2 eligible subrecipient. The tier structure is only applicable with regard to eligibility. OPSG funding allocations are based on the assessed border security risks as determined by the USBP.

3. Other Eligibility Criteria

National Incident Management System (NIMS) Implementation
Prior to allocation of any Federal preparedness awards in FY 2020, recipients must ensure and maintain adoption and implementation of NIMS. Detailed information on NIMS requirements are in the Preparedness Grants Manual.

Emergency Management Assistance Compact (EMAC) Membership
In support of the Goal, SHSP recipients must belong to, be in, or act as a temporary member of EMAC, except for American Samoa and the Commonwealth of the Northern Mariana Islands, which are not required to belong to EMAC at this time. All assets supported in part or entirely with FY 2020 HSGP funding must be readily deployable and NIMS-typed when possible to support emergency or disaster operations per existing EMAC agreements. In addition, funding may be used for the sustainment of core capabilities that, while they may not be physically deployable, support national response capabilities, such as Geographic/Geospatial Information Systems (GIS), interoperable communications systems, capabilities as defined under the Mitigation Mission Area of the Goal, and fusion centers.

Law Enforcement Terrorism Prevention Activities (LETPA)
Per section 2006 of the *Homeland Security Act of 2002*, as amended (6 U.S.C. § 607), DHS/FEMA is required to ensure that at least 25 percent of grant funding appropriated for grants awarded under HSGP's authorizing statute are used for law enforcement terrorism prevention activities. DHS/FEMA meets this requirement, in part, by requiring all recipients allocate at least 25 percent of the combined HSGP funds allocated under SHSP and UASI towards law enforcement terrorism prevention activities, as defined in 6 U.S.C. § 607. The LETPA allocation can be from SHSP, UASI, or both. The 25 percent LETPA allocation may be met by funding projects in any combination of the four national priority areas

identified above and any other investments. And the 25 percent LETPA allocation is in addition to the 80 percent pass-through requirement to local units of government and tribes, referenced below.

The National Prevention Framework describes those activities that should be executed upon the discovery of intelligence or information regarding an imminent threat to the homeland, to thwart an initial or follow-on terrorist attack and provides guidance to ensure the Nation is prepared to prevent, avoid, or stop a threatened or actual act of terrorism. Activities outlined in the National Prevention Framework are eligible for use as LETPA-focused funds. Also, where capabilities are shared with the protection mission area, the National Protection Framework activities are also eligible. All other terrorism prevention activities proposed for funding under LETPA must be approved by the FEMA Administrator.

4. Cost Share or Match

There is no cost share or match requirement for the FY 2020 HSGP.

D. Application and Submission Information

1. Key Dates and Times

a. Application Start Date: **February 14, 2020**

b. Application Submission Deadline: **April 15, 2020 at 5:00 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 the full application. **DHS/FEMA will not review applications that are received after the deadline or consider them for funding**. DHS/FEMA may, however, extend the application deadline on request for an 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, or other exigent or emergency circumstances.

Applicants experiencing technical issues must notify the FEMA Headquarters (HQ) Program Analyst prior to the application deadline. If applicants do not know their FEMA HQ Program Analyst or if there are programmatic 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, 9:00 a.m. – 5:00 p.m. ET.

c. Anticipated Funding Selection Date: *No later than* 7/1/2020

d. Anticipated Award Date: *No later than* 9/30/2020

e. Other Key Dates:

Event	Suggested Deadline for Completion
Obtain DUNS Number	3/1/2020
Obtain a valid Employer Identification Number (EIN)	3/1/2020
Update SAM registration	3/1/2020
Submit the initial application in Grants.gov	4/8/2020
Submit the final application in ND Grants	4/15/2020, 5:00 p.m. ET

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

See the Preparedness Grants Manual for information on requesting and submitting an application.

4. Steps Required to Submit an Application, Unique Entity Identifier, and System for Award Management (SAM)

To apply for an award under this program, all applicants must:

a. Apply for, update, or verify their Data Universal Numbering System (DUNS) Number from Dun & Bradstreet (D&B) and Employer ID Number (EIN)
b. In the application, provide a valid Data Universal Numbering System DUNS number, which is currently the unique entity identifier;
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;
a. Establish an Authorized Organizational Representative (AOR) in Grants.gov;
b. Submit an initial application in Grants.gov;
g. Submit the final application in the Non-Disaster Grants (ND Grants) system and
h. 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.

Applicants are advised that DHS may not make a federal award until the applicant has complied with all applicable DUNS and 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. See the Preparedness Grants Manual for additional information on the steps required to submit an application.

5. **Electronic Delivery**
   DHS/FEMA 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/FEMA requires applicants to submit their initial applications online through Grants.gov and to submit final applications through ND Grants.

6. **How to Register to Apply through Grants.gov**
   See the Preparedness Grants Manual for information on requesting and submitting an application.

7. **How to Submit an Initial Application to DHS/FEMA via Grants.gov**
   See the Preparedness Grants Manual for information on requesting and submitting an application.

8. **Timely Receipt Requirements and Proof of Timely Submission**
   As application submission is a two-step process, the applicant with the Authorized Organizational Representative (AOR) role who submitted the application will also receive an acknowledgement of receipt, a tracking number (in this format: GRANTXXXXXXXX) from Grants.gov, and an Agency Tracking Number (in this format: EMX-2020-XX-XXXX) with the successful transmission of the 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. All applications must be received in ND Grants by 5:00 p.m. ET on April 15, 2020. 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.

9. **Submitting the Final Application in Non-Disaster Grants System (ND Grants)**
   After submitting the initial application in Grants.gov, eligible applicants will be notified by DHS/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 but no later than **seven days before the application deadline**. Early registration will allow applicants to have adequate time to start and complete their application.

   In ND Grants applicants will be prompted to submit all of the information contained in the following forms. Applicants should review these forms before applying to ensure they have all the information required:
   - Standard Form 424A, Budget Information (Non-construction);
   - Standard Form 424B, Standard Assurances (Non-construction); and
   - Standard Form LLL, Disclosure of Lobbying Activities.

   In addition, applicants must submit copies of the following in ND Grants:
   - Investment Justification (the Investment Justification Template may be found in the Related Documents Tab of the Grants.gov posting and used as a preparation tool; responses to questions in the Template are entered into the GRT);

- List of Urban Area Working Group (UAWG) and Senior Advisory Committee (SAC) members;
- SAC charter;
- UAWG charter; and
- Indirect Cost Agreement, if the budget includes indirect costs and the applicant is required to have an indirect cost rate agreement. If the applicant is not required to have an indirect cost rate agreement but will charge indirect costs and is required to have an indirect cost rate proposal, the applicant must provide a copy of their indirect cost rate proposal with the application. See the section below on indirect costs for more information or contact the relevant Program Analyst or Grants Management Specialist for further instructions.

Applicants must submit copies of the following in ND Grants if applying for construction projects. The forms may be accessed in the Forms tab under SF-424 Family on Grants.gov:

- Standard Form 424C, Budget Information (Construction); and
- Standard Form 424D, Standard Assurances (Construction).

Applicants needing assistance registering for the ND Grants system should contact ndgrants@fema.gov or (800) 865-4076, Monday through Friday, 9 a.m. – 5 p.m. ET.

10. Content and Form of Application Submission

See the Preparedness Grants Manual for information on requesting and submitting an application.

HSGP Specific Application Instructions

Development of the Investment Justification (SHSP and UASI)

As part of the FY 2020 HSGP application process for SHSP and UASI funds, applicants must develop formal investment justifications (IJs) that address the proposed investments. Failure to fulfill of all of the terms contained in this section will be considered by DHS/FEMA in its evaluation of the effectiveness of the IJs in accordance with the Risk Methodology and Effectiveness Review described in the Application Review Information and may result in rejection of proposed investments or reduced funding allocations.

Each IJ must *demonstrate* how proposed investments:

- Support terrorism preparedness;
- Support closing capability gaps or sustaining capabilities identified in the community's THIRA/SPR process; and
- Support the overcoming of existing logistical, technological, legal, policy, and other impediments to collaborating, networking, sharing information, cooperating, and fostering a culture of national preparedness with federal, state, tribal, and local governments, as well as other regional, and nonprofit partners in efforts to prevent, prepare for, protect against, and respond to acts of terrorism, to meet its target capabilities, support the national security mission of DHS and other federal agencies, and to otherwise reduce the overall risk to the high-risk urban area, the State, or the Nation.

Each IJ must *explain* how the proposed investments will support the applicant's efforts to:

- Prevent a threatened or an actual act of terrorism;
- Prepare for all hazards and threats, while explaining the nexus to terrorism preparedness;
- Protect citizens, residents, visitors, and assets against the greatest threats and hazards, relating to acts of terrorism; and/or
- Respond quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of an act of terrorism or other catastrophic incidents.

Development of Investments and Projects (SHSP)

- Applicants must propose at least four and may include up to ten investments.
- Required national priority investment justifications must include the name of the priority in the investment name for easy identification.
- Within each investment in their IJ, applicants must propose at least one project to describe the activities they plan to implement with SHSP funds. There is no limit to the number of projects that may be submitted.
- Of the proposed SHSP-funded investments, one single project, within the required intelligence and information sharing investment, must be in support of a designated fusion center. Recipients must coordinate with the fusion center when developing a fusion center project prior to submission. See additional information on how to develop the fusion center projects below.
- Of the proposed SHSP-funded investments, one project in each of the required Cybersecurity and Soft Targets/Crowded Places investments must be in support of enhancing election security.
- All emergency communications investments must describe how such activities align with their Statewide Communication Interoperable Plan (SCIP). Recipients must coordinate with their Statewide Interoperability Coordinator (SWIC) and/or Statewide Interoperability Governance Body (SIGB) when developing an emergency communications investment prior to submission to ensure the project supports the statewide strategy to improve emergency communications and is compatible and interoperable with surrounding systems. The investment name must include the words "emergency communications" to easily identify any emergency communications investments.
- All requested funding must be associated with specific projects. For each project, several pieces of information must be provided to submit the project for consideration in the application, including the name of the project, the project description, the name of the subrecipient, if applicable, the recipient type (e.g., state or local), the project location (zip code of the primary location of the project), the primary core capability the project supports, whether the project activities are shareable and deployable, and which priority area (if any) the project is in support of. Projects should describe how the proposed investment supports closing capability gaps or sustaining capabilities identified in the THIRA/SPR process. Failure to fulfill of all of the terms contained in this section may be considered in the evaluation of the effectiveness of the IJs in accordance with the Risk Methodology and Effectiveness Review described in the Application Review Information and may result in rejection of proposed investments or reduced funding allocations.
- FEMA encourages states to use any DHS provided assessments, such as those performed

by DHS's Protective Security Advisors and Cybersecurity Advisors, when developing their investment justifications.

Priority Investments (SHSP)

States are encouraged to review the Strategic Framework for Countering Terrorism and Targeted Violence when developing investments.

Cybersecurity Investment Justification (5 percent)

At least one investment must be in support of the state's cybersecurity efforts. The investment must meet or exceed the FY 2020 national priority percentage for cybersecurity, and will also be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments, in order to receive a full allocation of SHSP funds. Cybersecurity investments must support the security and functioning of critical infrastructure and core capabilities as they relate to preventing, preparing for, protecting against, or responding to acts of terrorism. Recipients and subrecipients of FY 2020 HSGP grant awards will be required to complete the 2020 Nationwide Cybersecurity Review (NCSR), enabling agencies to benchmark and measure progress of improving their cybersecurity posture. The CIO, CISO or equivalent for each recipient should complete the NCSR. If there is no CIO or CISO, the most senior cybersecurity professional should complete the assessment. The NCSR is available at no cost to the user and takes approximately 2-3 hours to complete. The 2020 NCSR will be open from October – December 2020.

- The NCSR is an annual requirement for recipients and subrecipients of HSGP funds. Additionally, FEMA recognizes that some subawards will not be issued until after the NCSR has closed. In such cases, such subrecipients will be required to complete the first available NCSR offered after the subaward has been issued by the pass-through entity.
- Although not required by SLTTs that did not receive HSGP funds, all SLTT agencies with preparedness responsibilities are highly encouraged to participate and complete the NCSR to evaluate their cybersecurity posture. For detailed information and background on the NCSR, please see Information Bulletin 439.

In January 2017, the Department of Homeland Security designated the infrastructure used to administer the Nation's elections as critical infrastructure. This designation recognizes that the United States' election infrastructure is of such vital importance to the American way of life that its incapacitation or destruction would have a devastating effect on the country. Securing election infrastructure and ensuring an election free from foreign interference are national security priorities. Threats to election systems are constantly evolving, so defending these systems requires constant vigilance, innovation, and adaptation.

Given the importance of the Nation's election infrastructure, and the multiple and evolving threats to that infrastructure, at least one project within this investment must be in support of the state's efforts to enhance election security. Additional resources and information regarding election security are available through the Cybersecurity and Infrastructure Security Agency.

Soft Target Investment Justification (5 percent)
Soft targets and crowded places are increasingly appealing to terrorists and other extremist actors because of their relative accessibility and the large number of potential targets. This challenge is complicated by the prevalent use of simple tactics and less sophisticated attacks. Segments of our society are inherently open to the general public, and by nature of their purpose do not incorporate strict security measures. Given the increased emphasis by terrorists and other extremist actors to leverage less sophisticated methods to inflict harm in public areas, it is vital that the public and private sectors collaborate to enhance security of locations such as transportation centers, parks, restaurants, shopping centers, special event venues, and similar facilities.

Given the increased risk to soft targets and crowded places, at least one investment must be in support of the state's efforts to protect soft targets/crowded places. Additionally, the proposed investment must meet or exceed the FY 2020 national priority percentage for soft targets/crowded places and will also be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments in order to receive a full allocation of SHSP funds. Additional resources and information regarding securing soft targets and crowded places are available through the Cybersecurity and Infrastructure Security Agency. States are encouraged to engaged DHS' Protective Security Advisors' security assessments of soft targets to ensure that recommendations from those assessments are taken into consideration when allocating grant funding.

As noted above, given the importance of the Nation's election infrastructure, and the multiple and evolving threats to that infrastructure, at least one project within this investment must be in support of the state's efforts to enhance election security. Additional resources and information regarding election security are available through the Cybersecurity and Infrastructure Security Agency.

Information Sharing and Cooperation Investment Justification (5 percent)
Effective homeland security operations rely on timely information sharing and actionable intelligence to accurately assess and prevent threats against the United States. Accordingly, DHS works diligently to enhance intelligence collection, integration, analysis, and information sharing capabilities to ensure partners, stakeholders, and senior leaders receive actionable intelligence and information necessary to inform their decisions and operations. A critical and statutorily charged mission of DHS is to deliver intelligence and information to federal, state, local, and tribal governments and private sector partners. Cooperation and information sharing among state, federal, and local partners across all areas of the homeland security enterprise, including counterterrorism, cybersecurity, border security, immigration enforcement, and other areas is critical to homeland security operations and the prevention of, preparation for, protection against, and responding to acts of terrorism.

Given the importance of information sharing and collaboration to effective homeland security solutions, at least one investment must be in support of the state's efforts to enhance information sharing and cooperation with DHS and other federal agencies. As noted above, this requirement must include at least one dedicated fusion center project. Additional instructions on development of the fusion center project can be found below. Applicants must justify persuasively how they

will contribute to the information sharing and collaboration purposes of the investment and a culture of national preparedness, including how they will identify, address, and overcome any existing laws, policies, and practices that prevent information sharing. Additionally, the proposed investment must meet or exceed the FY 2020 national priority percentage for information sharing and cooperation with DHS, and will also be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments, in order to receive a full allocation of SHSP funds. Additional resources and information regarding collaboration and information sharing are available through the Department's Office of Intelligence and Analysis.

Emerging Threats Investment Justification (5 percent)

The spread of rapidly evolving and innovative technology, equipment, techniques, and knowledge presents new and emerging dangers for homeland security in the years ahead. Terrorists remain intent on acquiring weapons of mass destruction (WMD) capabilities, and rogue nations and non-state actors are aggressively working to develop, acquire, and modernize WMDs that they could use against the Homeland. Meanwhile, biological and chemical materials and technologies with dual use capabilities are more accessible throughout the global market. Due to the proliferation of such information and technologies, rogue nations and no-state actors have more opportunities to develop, acquire, and use WMDs than ever before. Similarly, the proliferation of unmanned aircraft systems, artificial intelligence, and biotechnology increase opportunities of threat actors to acquire and use these capabilities against the United States and its interests.

Given the increased risk of emerging threats, at least one investment must be in support of the state's efforts to address emerging threats. Additionally, the proposed investment must meet or exceed the FY 2020 national priority percentage for emerging threats, and will also be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments, in order to receive a full allocation of SHSP funds. Additional resources and information regarding emerging threats are available through the Countering Weapons of Mass Destruction Office and the Cybersecurity and Infrastructure Security Agency.

Development of Investments and Projects (UASI)

- Applicants must propose at least four and may include up to ten investments.
- Within each investment in their IJ, Urban Areas must propose at least one project to describe the activities they are planning to implement with UASI funds. There is no limit to the number of projects that may be submitted.
- Required national priority IJs must include the name of the priority in the investment name for easy identification.
- Of the proposed projects, Urban Areas are required to propose one single project, as part of the required intelligence and information sharing investment justification, in support of a designated fusion center within the Urban Area, if applicable. Recipients must coordinate with the fusion center when developing a fusion center project prior to submission. See additional information on how to develop fusion center investments below.
- Of the proposed UASI-funded investments, one project in each of the required Cybersecurity and Soft Targets/Crowded Places investments, must be in support of enhancing election security.

All emergency communications investments must describe how such activities align with their Statewide Communication Interoperable Plan (SCIP). Recipients must coordinate with their Statewide Interoperability Coordinator (SWIC) and/or Statewide Interoperability Governance Body (SIGB) when developing an emergency communications investment prior to submission to ensure the project supports the statewide strategy to improve emergency communications and is compatible and interoperable with surrounding systems. The investment name must include the words "emergency communications" to easily identify any emergency communications investments.

All requested funding must be associated with specific projects. For each project, several pieces of information must be provided to submit the project for consideration in the application, including the name of the project, the project description, the name of the subrecipient, if applicable, the recipient type (e.g., state or local), the project location (zip code of the primary location of the project), the primary core capability the project supports, whether the project activities are shareable and deployable, and which priority area (if any) the project is in support of. Projects should describe how the proposed investment supports closing capability gaps or sustaining capabilities identified in the THIRA/SPR process

Priority Investments - UASI

High-risk urban areas are encouraged to review the Strategic Framework for Countering Terrorism and Targeted Violence when developing investments.

Cybersecurity Investment Justification (5 percent)

At least one investment must be in support of the urban area's cybersecurity efforts. The investment must meet or exceed the FY 2020 national priority percentage for cybersecurity, and will also be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments, in order to receive a full allocation of UASI and SHSP funds. Cybersecurity investments must support the security and functioning of critical infrastructure and core capabilities as they relate to preventing, preparing for, protecting against, or responding to acts of terrorism. Recipients and subrecipients of FY 2020 HSGP awards will be required to complete the 2020 Nationwide Cybersecurity Review (NCSR), enabling agencies to benchmark and measure progress of improving their cybersecurity posture. The CIO, CISO or equivalent for each recipient should complete the NCSR. If there is no CIO or CISO, the most senior cybersecurity professional should complete the assessment. The NCSR is available at no cost to the user and takes approximately 2- 3 hours to complete. The 2020 NCSR will be open from October – December 2020.

- The NCSR is an annual requirement for recipients and subrecipients of HSGP funds. Additionally, FEMA recognizes that some subawards will not be issued until after the NCSR has closed. In such cases, such subrecipients will be required to complete the first available NCSR offered after the subaward has been issued by the pass-through entity.
- Although not required by SLTTs that did not receive HSGP funds, all SLTT agencies with preparedness responsibilities are highly encouraged to participate and complete the NCSR to evaluate their cybersecurity posture. For detailed information and background on the NCSR, please see Information Bulletin 439.

In January 2017, the Department of Homeland Security designated the infrastructure used to administer the Nation's elections as critical infrastructure. This designation recognizes that the United States' election infrastructure is of such vital importance to the American way of life that its incapacitation or destruction would have a devastating effect on the country. Securing election infrastructure and ensuring an election free from foreign interference are national security priorities. Threats to election systems are constantly evolving, so defending these systems requires constant vigilance, innovation, and adaptation.

Given the importance of the Nation's election infrastructure, and the multiple and evolving threats to that infrastructure, at least one project within this investment must be in support of the state's efforts to enhance election security. Additional resources and information regarding election security are available through the Cybersecurity and Infrastructure Security Agency.

Soft Target Investment Justification (5 percent)
Soft targets and crowded places are increasingly appealing to terrorists and other extremist actors because of their relative accessibility and the large number of potential targets. This challenge is complicated by the prevalent use of simple tactics and less sophisticated attacks. Segments of our society are inherently open to the general public, and by nature of their purpose do not incorporate strict security measures. Given the increased emphasis by terrorists and other extremist actors to leverage less sophisticated methods to inflict harm in public areas, it is vital that the public and private sectors collaborate to enhance security of locations such as transportation centers, parks, restaurants, shopping centers, special event venues, and similar facilities.

Given the increased risk to soft targets and crowded places, at least one investment must be in support of the urban area's efforts to protect soft targets/crowded places. Additionally, the proposed investment must meet or exceed the FY 2020 national priority percentage for soft targets/crowded places and will also be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments, in order to receive a full allocation of UASI funds. Additional resources and information regarding securing soft targets and crowded places are available through the Cybersecurity and Infrastructure Security Agency.

As noted above, given the importance of the Nation's election infrastructure, and the multiple and evolving threats to that infrastructure, at least one project within this investment must be in support of the state's efforts to enhance election security. Additional resources and information regarding election security are available through the Cybersecurity and Infrastructure Security Agency.

Information Sharing and Cooperation Investment Justification (5 percent)
Effective homeland security operations rely on timely information sharing and actionable intelligence to accurately assess and prevent threats against the United States. Accordingly, DHS works diligently to enhance intelligence collection, integration, analysis, and information sharing capabilities to ensure partners, stakeholders, and senior leaders receive actionable intelligence and information necessary to inform their decisions and operations. A critical and statutorily charged mission of DHS is to deliver intelligence and information to federal, state, local, and tribal governments and private sector partners. Cooperation and information sharing among state, federal, and local partners across all areas of the homeland security enterprise, including counterterrorism, cybersecurity, border security, immigration enforcement, and other areas is

critical to homeland security operations and the prevention of, preparation for, protection against, and responding to acts of terrorism.

Given the importance of information sharing and collaboration to effective homeland security solutions, at least one investment must be in support of the urban area's efforts to enhance information sharing and cooperation with DHS and other federal agencies. As noted above, this requirement must include at least one dedicated fusion center project. Additional instructions on development of the fusion center project can be found below. Applicants must justify persuasively how they will contribute to the information sharing and collaboration purposes of the investment and a culture of national preparedness, including how they will identify, address, and overcome any existing laws, policies, and practices that prevent information sharing. Additionally, the proposed investment must meet or exceed the FY 2020 national priority percentage for information sharing and cooperation with DHS, and will also be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments, in order to receive a full allocation of UASI funds. Additional resources and information regarding collaboration and information sharing are available through the Department's Office of Intelligence and Analysis.

Emerging Threats Investment Justification (5 percent)
The spread of rapidly evolving and innovative technology, equipment, techniques, and knowledge presents new and emerging dangers for homeland security in the years ahead. Terrorists remain intent on acquiring weapons of mass destruction (WMD) capabilities, and rogue nations and non-state actors are aggressively working to develop, acquire, and modernize WMDs that they could use against the Homeland. Meanwhile, biological and chemical materials and technologies with dual use capabilities are more accessible throughout the global market. Due to the proliferation of such information and technologies, rogue nations and non-state actors have more opportunities to develop, acquire, and use WMDs than ever before. Similarly, the proliferation of unmanned aircraft systems, artificial intelligence, and biotechnology increase opportunities of threat actors to acquire and use these capabilities against the United States and its interests.

Given the increased risk of emerging threats, at least one investment must be in support of the urban area's efforts to address emerging threats. Additionally, the proposed investment must meet or exceed the FY 2020 national priority percentage for emerging threats, and will also be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments, in order to receive a full allocation of UASI funds. Additional resources and information regarding emerging threats are available through the Countering Weapons of Mass Destruction Office and the Cybersecurity and Infrastructure Security Agency.

Development of Fusion Center Projects (SHSP and UASI)
If applicable, each applicant must identify a fusion center project that will:

- Indicate alignment to a designated Fusion Center.
- Provide both a brief narrative description and funding itemization for the proposed project activities that directly support the designated fusion center.
- The descriptive narrative and the financial itemization should align improvement or sustainment requests with fusion center activities as they relate to the Fusion Center Performance Measures found in the Preparedness Grants Manual.

- If the project description and funding itemization do not directly support the fusion center or clearly align to the Fusion Center Performance Measures, then the project may be conditionally approved until a Fusion Center Addendum is submitted.

Sample Fusion Center Funding Itemization
A sample project description and funding itemization are below. For the itemized projects, clearly identify the anticipated fusion center performance improvement or sustainment as a result of the proposed funding.

The X Fusion enhancement project will fund:
- *Salaries, benefits, and training for X number of Fusion Center intelligence analysts*
- *Travel costs associated with fusion center analyst training.*
- *This project will directly sustain the Center's current capabilities and performance and directly aligns with performance measures 2020.XXX.*
- *We anticipate seeing an improvement in the quality and quantity of analytic production and responses to requests for information as a direct result of the funding of this project.*

The funding itemization for a fusion center project should include the amount and percent of each relevant solution area. As an example:

Solution Area and Amount of Proposed Funding		***Percent of Proposed Funding***
Planning:	*$10,000.00*	*2%*
Organization:	*$200,000*	*48%*
Equipment:	*$200,000*	*48%*
Training:	*$10,000*	*2%*
Exercises:	*$0*	*0%*
Total:	*$420,000*	*100%*

Completing IJs in the Grant Reporting Tool (GRT) (SHSP and UASI)
In the Related Documents section of the Grants.gov posting, applicants can find the IJ template and instructions for collecting the required information for investments and projects. Additionally, applicants should utilize the Project Worksheet located in Grants.gov posting to assemble the information required for each project, which will facilitate the input of that information into the GRT.

Development of Concept of Operations for OPSG
As part of the FY 2020 OPSG application process, each eligible local unit of government at the county or Federally recognized tribal government level must develop a strategic plan called a Concept of Operations (CONOP)/Application, which is a formal proposal of action to address a specific situation and forms the basis for Operations Orders, in coordination with state and Federal law enforcement agencies, to include, but not limited to CBP/USBP. CONOPs that are developed at the county level should be inclusive of city, county, tribal, and other local law enforcement agencies that are eligible to participate in OPSG operational activities, and the CONOP/Application should describe participating agencies in the Executive Summary. CONOP/Application details should include the names of the agencies, points of contact, and individual funding requests. All CONOPs/Applications must be developed in collaboration with

the local USBP sector office, the SAA and the local unit of government. Requests for funding in CONOPs/Applications must be based on risks and the operational enforcement support requirements of its corresponding USBP Sector, as well as the national priorities identified below. USBP Sector offices will forward the CONOPs to USBP Headquarters for vetting and coordination. Applicants will forward corresponding OPSG Applications to the SAA for submission to FEMA. USBP Headquarters will reconcile all submitted CONOPs with the OPSG Applications. FEMA will review and evaluate all CONOPs and OPSG Applications and funding will be allocated based on the review and selection criteria identified in this NOFO.

OPSG Applicants will be required to clearly articulate and identify how the CONOPs will address the national priorities identified below.

Information Sharing and Cooperation
Effective border security operations rely on timely information sharing and actionable intelligence to accurately assess and prevent threats against the United States. Accordingly, DHS works diligently to enhance intelligence collection, integration, analysis, and information sharing capabilities to ensure partners, stakeholders, and senior leaders receive actionable intelligence and information necessary to inform their decisions and operations. A critical and statutorily charged mission of DHS is to deliver intelligence and information to federal, state, local, and tribal governments and private sector partners. Cooperation and information sharing among state, federal, and local partners across all areas of the homeland security enterprise, including counterterrorism, cybersecurity, border security, immigration enforcement, and other areas is critical to homeland security operations and the prevention of, preparation for, protection against, and responding to acts of terrorism.

Given the importance of information sharing and collaboration to effective homeland security solutions, the CONOP must be in support of the recipient's efforts to enhance information sharing and cooperation with DHS and other federal agencies. Applicants must justify persuasively how they will contribute to the information sharing and collaboration purposes of the OPSG program and a culture of national preparedness, including how they will identify, address, and overcome any existing laws, policies, and practices that prevent information sharing. Additional resources and information regarding collaboration and information sharing are available through the Department's Office of Intelligence and Analysis.

Emerging Threats
The spread of rapidly evolving and innovative technology, equipment, techniques, and knowledge presents new and emerging dangers for homeland security in the years ahead. Terrorists remain intent on acquiring weapons of mass destruction (WMD) capabilities, and rogue nations and non-state actors are aggressively working to develop, acquire, and modernize WMDs that they could use against the Homeland. Meanwhile, biological and chemical materials and technologies with dual use capabilities are more accessible throughout the global market. Due to the proliferation of such information and technologies, rogue nations and non-state actors have more opportunities to develop, acquire, and use WMDs than ever before. Similarly, the proliferation of unmanned aircraft systems, artificial intelligence, and biotechnology increase opportunities of threat actors to acquire and use these capabilities against the United States and its interests.

Given the increased risk of emerging threats, the CONOP must be in support of the recipient's efforts to address emerging threats. Additional resources and information regarding emerging threats are available through the Countering Weapons of Mass Destruction Office and the Cybersecurity and Infrastructure Security Agency.

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/2017/11/SPOC-Feb.-2018.pdf.

12. Funding Restrictions
Federal funds made available through this award may be used for the purpose set forth in this award and must be consistent with the statutory authority for the award. Award funds may not be used for matching funds for any other Federal awards, 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. See the Preparedness Grants Manual for more information on funding restrictions.

13. Environmental Planning and Historic Preservation (EHP) Compliance
See the Preparedness Grants Manual for information on EHP Compliance.

14. Emergency Communications Investments
If an entity uses HSGP 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:

- Applicants must describe in the investment how proposed communications investments align to needs identified in their SCIP. Effective project alignment will require advance coordination with the SWIC and consultation with governing bodies such as the SIGB or Statewide Interoperability Executive Committee (SIEC), as they serve as the primary steering group for the statewide interoperability strategy. Additionally, recipients should consult subject matter experts serving on governance bodies, such as broadband experts, chief information officers, representatives from utilities, or legal and financial experts, when developing proposals.
- The signatory authority for the SAA must certify in writing to DHS/FEMA their compliance with the *SAFECOM Guidance*. The certification letter should be coordinated with the SWIC for each state and must be uploaded to ND Grants at the time of the first Program Performance Report (PPR) submission.
- All states and territories must designate a full-time SWIC who has the authority and resources to actively improve interoperability with emergency management and response agencies across all levels of government, to include establishing statewide plans, policies, and procedures, and coordinating decisions on communications investments funded through Federal grants. Note that the designated full-time SWIC may also be the state's or territory's cybersecurity point of contact. SWIC status information will be maintained by the DHS Office of Emergency Communications and will be verified by FEMA GPD through programmatic monitoring activities.
- By the period of performance end date, all states and territories must update the SCIP, with a focus on communications resilience/continuity, to include assessment and

mitigation of all potential risks identified in the SCIP: natural disasters, accidental damage (human failures), intentional damage (sabotage, terrorism), cybersecurity, etc. Following the initial update, the SCIP should be updated on an annual basis. SCIP status information will be maintained by the DHS Office of Emergency Communications and will be verified by FEMA GPD through programmatic monitoring activities.

All states and territories must test their emergency communications capabilities and procedures (as outlined in their operational communications plans) in conjunction with regularly planned exercises (separate/addition emergency communications exercises are not required) and must submit an After Action Report/Improvement Plan (AAR/IP) to the Homeland Security Exercise and Evaluation Program's (HSEEP) electronic message inbox at hseep@fema.gov within 90 days of exercise completion. Exercises should be used to both demonstrate and validate skills learned in training and to identify gaps in capabilities. Resilience and continuity of communications should be tested during training and exercises to the greatest extent possible. Further, exercises should include participants from multiple jurisdictions, disciplines, and levels of government and include emergency management, emergency medical services, law enforcement, interoperability coordinators, public health officials, hospital officials, officials from colleges and universities, and other disciplines and private sector entities, as appropriate. Findings from exercises should be used to update programs to address gaps in emergency communications as well as emerging technologies, policies, and partners. Recipients are encouraged to increase awareness and availability of emergency communications exercise opportunities across all levels of government.

States, territories, and other eligible grant recipients are advised that HSGP funding may be used to support communications planning (including the cost of hiring a SWIC, participation in governance bodies and requirements delineated above), training, exercises, and equipment costs. Costs for transitioning to the FirstNet network may also be eligible. More information regarding FirstNet can be found in the Preparedness Grants Manual.

15. Detailed Budget

Applicants must provide budget summary worksheets for all funds requested at the time of application. The budget summary worksheets must be complete, reasonable, and cost-effective in relation to the proposed project and should provide the basis of computation of all project-related costs (including management and administrative costs) and any appropriate narrative. FEMA must be able to thoroughly evaluate the projects being submitted based on the information provided. FEMA must be able to determine how much funding is being used by the direct recipient for projects carried out by the direct recipient and how much funding is being passed through to sub-recipients for each sub-program (UASI, SHSP, OPSG). Consequently, applicants must provide an appropriate level of detail within the budget summary worksheets to clarify what will be purchased and spent. Sample budget summary worksheets are available on the grants.gov posting for the HSGP in the Related Documents tab and may be used as a guide to assist applicants in the preparation of budgets and budget narratives.

16. Funds Transfer Restriction

The recipient is prohibited from transferring funds between programs (includes the SHSP, the UASI, and OPSG). Recipients can submit an investment/project where funds come from multiple funding sources (e.g., the SHSP and UASI), however, recipients are not allowed to

divert funding from one program to another due to the risk-based funding allocations, which were made at the discretion of DHS/FEMA.

17. 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 Authorized Representative 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.

18. Cost Principles
Costs charged to this award must be consistent with the Cost Principles for Federal Awards located at 2 C.F.R. Part 200, Subpart E. For more information on 2 C.F.R. Part 200, please refer to FEMA GPD Information Bulletin 400, *FEMA's Implementation of 2 C.F.R. Part 200, the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* ("Super Circular" or "Omni Circular").

19. Direct Costs

a. Planning
Planning costs are allowed under this program.

b. Organization
Organization costs are allowed under this program.

c. Equipment
Equipment costs are allowed under this program.

d. Training
Training costs are allowed under this program.

e. Exercises
Exercise costs are allowed under this program.

f. Personnel
Personnel hiring, overtime, and backfill expenses are permitted under this grant to perform allowable HSGP planning, organization, training, exercise, and equipment activities. Under OPSG, overtime costs are allowable only in so far as they meet the intent of the program. All recipients and subrecipients of HSGP funds, including SHSP, UASI, and OPSG allocations, may not use more than 50 percent of their awards to pay for personnel activities unless a waiver is approved by FEMA. For more information on the 50 percent personnel cap, please see FEMA Information Bulletin (IB) 421, Clarification on the *Personnel Reimbursement for Intelligence Cooperation and Enhancement of Homeland Security Act of 2008* (Public Law 110-412) – the PRICE Act.

g. Operational Overtime
Operational overtime costs are allowed under this program. Prior to use of funds for operational overtime, recipients must receive approval from DHS/FEMA.

h. Travel

Domestic travel costs are allowed under this program, as provided for in this NOFO. International travel is not an allowable cost under this program unless approved in advance by DHS/FEMA.

i. Construction and Renovation

Construction and renovation costs to achieve capability targets related to preventing, preparing for, protecting against, or responding to acts of terrorism are allowed under this program. For construction and renovation costs to be allowed, they must be specifically approved by DHS/FEMA in writing prior to the use of any program funds. Applicants must use the EHP approval process. Limits on the total amount of grant funding that may be used for construction or renovation may apply. Additionally, recipients are required to submit Standard Form 424C.

j. Maintenance and Sustainment

Maintenance- and sustainment-related costs, such as maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees, are allowable as described in FP 205-402-125-1, Maintenance Contracts and Warranty Coverage Funded by Preparedness Grants Policy (http://www.fema.gov/media-library/assets/documents/32474).

k. Management and Administration (M&A) Costs

Management and administration (M&A) activities are those directly relating to the management and administration of HSGP funds, such as financial management and monitoring. A maximum of up to five percent of HSGP funds awarded may be retained by the state, and any funds retained are to be used solely for M&A purposes associated with the HSGP 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 HSGP award.

Recipients or subrecipients may apply or credit M&A funding toward the recipient's requirement to allocate funding toward the four national priority areas. For example, if a recipient spends $5,000 to manage or administer its funding dedicated toward its enhancing cybersecurity investment, the recipient may credit that funding toward its requirement to allocate at least 5 percent of its award to enhancing cybersecurity.

A state's HSGP funds for M&A calculation purposes includes the total of its SHSP, UASI, and OPSG awards. While the SAA 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 each HSGP program. To meet this requirement, the percentage of SHSP and UASI funds passed through to local or tribal jurisdictions must be based on the state's total HSGP award prior to withholding any M&A.

In retaining these funds, states may retain a maximum of 2.5 percent of the OPSG allocation, which must be withheld from the pass-through to each subrecipient county or tribe in an equal percentage. The SAA may also retain additional funding from its SHSP award to manage and administer the OPSG award, but that additional amount is also capped at an amount equal to 2.5 percent of the OPSG award. Examples applying this principle:

SAA 1:
SHSP: $1,000,000
OPSG: $2,500,000
UASI: $2,500,000
M&A Maximum: $300,000 (5 percent of $6,000,000)
Maximum M&A for SHSP = $50,000
Maximum M&A for OPSG = $125,000. Of that amount, $62,500 (2.5 percent) may be retained from the OPSG allocation, and the other $62,500 would come from the SHSP allocation. Any amount used to manage and administer OPSG that is charged to SHSP may be above and beyond the $50,000 available to manage the SHSP allocation.

SAA 2:
SHSP: $3,500,000
OPSG: $1,000,000
M&A Maximum: $225,000 (5 percent of $4,500,000)
Maximum M&A for SHSP: $175,000
Maximum M&A for OPSG = $50,000. Of that amount, $25,000 (2.5 percent) may be retained from the OPSG allocation, and the other $25,000 would come from the SHSP allocation. Any amount used to manage and administer OPSG that is charged to SHSP may be above and beyond the $175,000 available to manage the SHSP allocation.

Please note, Information Bulletin (IB) 365: Management and Administration Costs in the Homeland Security and DHS/FEMA Policy 207-087-1, which can be found at http://www.fema.gov/library/viewRecord.do?id=7837, **do not apply to awards made in FY 2020 under this NOFO**. The IB and Policy remain in effect for all previous awards.

L. Critical Emergency Supplies
Critical emergency supplies are allowed under this program.

M. Secure Identification
Secure Identification costs are allowed under this program.

N. 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 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. 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. 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.

O. General Purpose Equipment
HSGP allows expenditures on general purpose equipment if it aligns to and supports one or more core capabilities identified in the Goal and has a nexus to terrorism preparedness. General purpose equipment, like all equipment funded under the HSGP, must be sharable through the

Emergency Management Assistance Compact (EMAC)[3] and allowable under 6 U.S.C. § 609, and any other applicable provision of the *Homeland Security Act of 2002*, as amended. Examples of such general-purpose equipment may include:

- Law enforcement vehicles;
- Emergency medical services (EMS) equipment and vehicles;
- Fire service equipment and vehicles, to include hose, pump accessories, and foam concentrate for specialized chemical, biological, radiological, nuclear, and explosives (CBRNE) response;
- Interoperability of data systems, such as computer aided dispatch (CAD) and record management systems (RMS); and
- Office equipment for staff[4] engaged in homeland security program activity.

Equipment allowability is based on the Authorized Equipment List (AEL) but exceptions may be considered on a case-by-case basis if (1) the equipment identified to be purchased directly maps to a core capability contained within the Goal, and (2) the equipment's purpose (when operational) falls under the permitted use of funds in accordance with 6 U.S.C. § 609, and any other applicable provision of the *Homeland Security Act of 2002*, as amended.

P. Allowable Cost Matrix

The following matrix provides allowable cost activities that fall under each of the cost categories noted above. Recipients and subrecipients must follow all applicable requirements in 2 C.F.R. Part 200 (*Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*). Funds under HSGP may be used to cover the costs for evaluating the impact of these grants on the state or urban area's core capabilities and capability gaps. This list is not exhaustive, therefore, if there are any questions regarding allowable costs, please contact the appropriate HQ GPD Program Analyst. For additional information on allowable costs, see the Preparedness Grants Manual.

Allowable Program Activities	SHSP	UASI	OPSG
Allowable Planning Costs			
Developing hazard/threat-specific annexes	Y	Y	N
Developing and implementing homeland security support programs and adopting ongoing DHS/FEMA national initiatives	Y	Y	N
Developing related terrorism and other catastrophic event prevention activities	Y	Y	N
Developing and enhancing plans and protocols	Y	Y	N
Developing or conducting assessments	Y	Y	N
Hiring of full- or part-time staff or contract/consultants to assist with planning activities	Y	Y	N
Materials required to conduct planning activities	Y	Y	N
Travel/per diem related to planning activities	Y	Y	Y
Overtime and backfill costs (in accordance with operational Cost Guidance)	Y	Y	Y
Issuance of WHTI-compliant Tribal identification cards	Y	N	N
Activities to achieve planning inclusive of people with disabilities and others with access and functional needs and limited English proficiency.	Y	Y	N

[3] Except for American Samoa and the Commonwealth of the Northern Mariana Islands, which are not required to belong to EMAC at this time.

[4] This applies to all homeland security personnel and is not limited to management and administration staff, and costs are to be captured outside the cap on management and administration costs

Allowable Program Activities	SHSP	UASI	OPSG
Coordination with Citizen Corps Councils for public information/education and development of volunteer programs	Y	Y	N
Update governance structures and processes and plans for emergency communications	Y	Y	N
Development, and review and revision of continuity of operations plans	Y	Y	N
Development, and review and revision of the THIRA/SPR continuity of operations plans	Y	Y	N
Allowable Organizational Activities **Note:** Personnel hiring, overtime, and backfill expenses are permitted under this grant only to the extent that such expenses are for the allowable activities within the scope of the grant.			
Program management	Y	Y	N
Development of whole community partnerships	Y	Y	N
Structures and mechanisms for information sharing between the public and private sector	Y	Y	N
Implementing models, programs, and workforce enhancement initiatives	Y	Y	N
Tools, resources, and activities that facilitate shared situational awareness between the public and private sectors	Y	Y	N
Operational support	Y	Y	N
Utilization of standardized resource management concepts	Y	Y	N
Responding to an increase in the threat level under the National Terrorism Advisory System (NTAS), or needs in resulting from a National Special Security Event	Y	Y	N
Reimbursement for select operational expenses associated with increased security measures at critical infrastructure sites incurred (up to 50 percent of the allocation)	Y	Y	Y
Overtime for information, investigative, and intelligence sharing activities (up to 50 percent of the allocation)	Y	Y	Y
Hiring of new staff positions/contractors/consultants for participation in information/intelligence analysis and sharing groups or fusion center activities (up to 50 percent of the allocation).	Y	Y	Y
Allowable Equipment Categories			
Personal Protective Equipment	Y	Y	Y
Allowable Equipment Categories			
Explosive Device Mitigation and Remediation Equipment	Y	Y	N
CBRNE Operational Search and Rescue Equipment	Y	Y	N
Information Technology	Y	Y	Y
Cybersecurity Enhancement Equipment	Y	Y	N
Interoperable Communications Equipment	Y	Y	Y
Detection	Y	Y	Y
Decontamination	Y	Y	N
Medical countermeasures	Y	Y	Y
Power (e.g., generators, batteries, power cells)	Y	Y	Y
CBRNE Reference Materials	Y	Y	N
CBRNE Incident Response Vehicles	Y	Y	N
Terrorism Incident Prevention Equipment	Y	Y	Y
Physical Security Enhancement Equipment	Y	Y	Y
Inspection and Screening Systems	Y	Y	Y
Animal Care and Foreign Animal Disease	Y	Y	N
CBRNE Prevention and Response Watercraft	Y	Y	N
CBRNE Prevention and Response Unmanned Aircraft	Y	Y	N
CBRNE Aviation Equipment	Y	Y	N
CBRNE Logistical Support Equipment	Y	Y	N
Intervention Equipment (e.g., tactical entry, crime scene processing)	Y	Y	Y
Critical emergency supplies	Y	Y	N
Vehicle acquisition, lease, and rental	N	N	Y
Other Authorized Equipment	Y	Y	Y

Allowable Program Activities	SHSP	UASI	OPSG
Allowable Training Costs			
Overtime and backfill for emergency preparedness and response personnel attending DHS/FEMA-sponsored and approved training classes	Y	Y	N
Overtime and backfill expenses for part-time and volunteer emergency response personnel participating in DHS/FEMA training	Y	Y	N
Training workshops and conferences	Y	Y	Y
Activities to achieve training inclusive of people with disabilities and others with access and functional needs and limited English proficiency	Y	Y	N
Full- or part-time staff or contractors/consultants	Y	Y	Y
Travel	Y	Y	Y
Supplies	Y	Y	N
Instructor certification/re-certification	Y	Y	N
Coordination with Citizen Corps Councils in conducting training exercises	Y	Y	N
Interoperable communications training	Y	Y	N
Activities to achieve planning inclusive of people with limited English proficiency	Y	Y	N
Immigration enforcement training	Y	Y	Y
Allowable Exercise Related Costs			
Design, Develop, Conduct, and Evaluate an Exercise	Y	Y	N
Full- or part-time staff or contractors/consultants	Y	Y	N
Overtime and backfill costs, including expenses for part-time and volunteer emergency response personnel participating in DHS/FEMA exercises	Y	Y	N
Implementation of HSEEP	Y	Y	N
Activities to achieve exercises inclusive of people with disabilities and others with access and functional needs	Y	Y	N
Travel	Y	Y	N
Supplies	Y	Y	N
Interoperable communications exercises	Y	Y	N
Allowable Exercise Related Costs			
Activities to achieve planning inclusive of people with limited English proficiency	Y	Y	N
Allowable Management & Administrative Costs			
Hiring of full- or part-time staff or contractors/consultants to assist with the management of the respective grant program, application requirements, and compliance with reporting and data collection requirements	Y	Y	Y
Development of operating plans for information collection and processing necessary to respond to DHS/FEMA data calls	Y	Y	Y
Overtime and backfill costs	Y	Y	Y
Travel	Y	Y	Y
Meeting related expenses	Y	Y	Y
Authorized office equipment	Y	Y	Y
Recurring expenses such as those associated with cell phones and faxes during the PoP of the grant program	Y	Y	N
Leasing or renting of space for newly hired personnel during the PoP of the grant Program	Y	Y	N
Law Enforcement Terrorism Prevention Activities (LETPA) Costs			
Integration and interoperability of systems and data, such as CAD and RMS, to facilitate the collection,	Y	Y	N
Maturation and enhancement of designated state and major Urban Area fusion centers	Y	Y	N
Coordination between fusion centers and other analytical and investigative efforts	Y	Y	N

Allowable Program Activities	SHSP	UASI	OPSG
Implementation and maintenance of the Nationwide SAR Initiative	Y	Y	N
Implementation of the "If You See Something, Say Something®" campaign	Y	Y	N
Increase physical security, through law enforcement personnel and other protective measures, by implementing preventive and protective measures at critical	Y	Y	N
Building and sustaining preventive radiological and nuclear detection capabilities	Y	Y	N

E. Application Review Information

1. Application Evaluation Criteria

a. Programmatic Criteria

Allocations

Risk Methodology and Effectiveness Review
The risk methodology and effectiveness review first determine the relative risk of terrorism faced by a given area considering the potential risk of terrorism to people, critical infrastructure, and economic security. The analysis includes, but is not limited to, threats from violent domestic extremists, international terrorist groups, and individuals inspired by terrorists abroad. See the Preparedness Grants Manual and Application Evaluation Criteria for additional information on risk methodology and effectiveness review.

The second part of the risk methodology and effectiveness review determines whether the proposed project is clear, logical, and reasonable to address the priority area of interest and contribute to a culture of national preparedness. This part considers factors such as how well the project is described and how well the project addresses the objectives and strategies of the priority area.

Risk and effectiveness will be given equal consideration in determining final award amounts.

NOTE: The THIRA/SPR process is separate from the risk methodology and effectiveness review, and its results do not affect grant allocations.

Evaluation Criteria
FEMA will evaluate the FY 2020 HSGP applications for completeness, adherence to programmatic guidelines, and anticipated effectiveness of the proposed investments. FEMA's review will include verification that each IJ or project:

- Meets the national priority required spend percentages.
- Aligns with at least one core capability identified in the Goal;
- Demonstrates how investments support closing capability gaps or sustaining capabilities identified in the THIRA/SPR process; and
- Supports a NIMS-typed resource and whether those assets are deployable/shareable to support emergency or disaster operations per existing EMAC agreements.

In addition to the above, FEMA will determine whether the proposed approach is clear, logical, and reasonable to address the priority areas of interest and contribute to a culture of national preparedness. This part considers factors such as the objectives and strategies proposed to address the priority area, how the objectives and strategies overcome legal, political, or practical obstacles to reduce overall risk, the process and criteria to select additional relevant projects, and the approach to monitor awards to satisfy the funding percentage allocations. Effectiveness will be evaluated prior to award and may impact the final overall award amount. To that end, IJs should include:

- How the proposed investment addresses the national priority;
- An explanation of how the proposed projects were selected and will achieve objectives and strategies to build or sustain the core capability gaps identified in the SPR, including expected long-term impact where applicable;
- A summary of laws, policies and practices that can be enhanced, eliminated, or otherwise changed in order to achieve the goals of the project and foster a culture of national preparedness;
- A summary of the collaboration efforts to prevent, prepare for, protect against, and respond to acts of terrorism as well as anticipated outcomes of the project.

For FY 2020 HSGP applications, effectiveness will be evaluated based on the following five factors:

- Investment Strategy (30%): Proposals will be evaluated based on the quality and extent to which applicants describe an effective strategy that demonstrates that proposed projects support the program objective of preventing, preparing for, protecting against, and responding to acts of terrorism, to meet its target capabilities, and otherwise reduce the overall risk to the high-risk urban area, the State, or the Nation.

- Budget (10%): Proposals will be evaluated based on the extent to which applicants describe a budget plan for each investment demonstrating how the applicant will maximize cost effectiveness of grant expenditures.

- Impact/Outcomes (30%): Proposals will be evaluated on how this investment helps the jurisdiction close capability gaps identified in its Stakeholder Preparedness Review and addresses national priorities outlined in the FY 2020 NOFO. Further, proposals will be evaluated on their identification and estimated improvement of core capability(ies), theassociated standardized target(s) that align with their proposed investment, and the ways in which the applicant will measure and/or evaluate improvement.

- Collaboration (30%): Proposals will be evaluated based on the degree to which the proposal adequately details how the recipient will use investments and other means to overcome existing logistical, technological, legal, policy, and other impediments to collaborating, networking, sharing information, cooperating, and fostering a culture of national preparedness with federal, state, tribal, and local governments, as well as other regional and nonprofit partners in efforts to prevent, prepare for, protect against, and respond to acts of terrorism, to meet its target capabilities, support the national security mission of DHS and other federal agencies, and to otherwise reduce the overall risk to the high-risk urban area, the State, or the Nation. In evaluating applicants under this factor FEMA will consider the information provided by the applicant and may also consider relevant information from other sources.

- Past Performance (additional consideration): Proposals will be evaluated based on the

applicants demonstrated capability to execute the proposed investments. In evaluating applicants under this factor FEMA will consider the information provided by the applicant and may also consider relevant information from other sources.

Recipients are expected to conform, as applicable, with accepted engineering practices, established codes, standards, modeling techniques, and best practices, and participate in the development of case studies demonstrating the effective use of grant funds, as requested.

Review and Selection Process (SHSP and UASI)
To ensure the effectiveness of proposed investments and projects, all applications will undergo a Federal review as described herein. The Federal review will be conducted by DHS and FEMA. IJs will be reviewed at both the investment and project level. Results of the effectiveness analysis may result in a recipient receiving a reduced grant award.

Cybersecurity investments will be reviewed by DHS/FEMA, CISA, and other DHS components as appropriate, for compliance with purposes and requirements of the priority investment area. Proposed investments will be reviewed for effectiveness using the criteria set forth in this NOFO.

Soft Targets/Crowded Places investments will be reviewed by DHS/FEMA, CISA, and other DHS components as appropriate, for compliance with purposes and requirements of the priority investment area. Proposed investments will be reviewed for effectiveness using the criteria set forth in this NOFO.

Information Sharing and Cooperation Investments will be reviewed by DHS/FEMA, DHS Intelligence and Analysis, and other DHS components as appropriate, for compliance with purposes and requirements of the priority investment area. Proposed investments will be reviewed for effectiveness using the criteria set forth in this NOFO.

As part of the above, Fusion center projects will be reviewed by DHS/FEMA for compliance with HSGP NOFO requirements to prioritize the alignment of requests with results from the annual Fusion Center Assessment Program. If a fusion center investment does not meet the requirements, a Fusion Center Addendum must be completed and submitted for review and approval prior to expending funds allocated to fusion center activities.

Emerging threats investments will be reviewed by DHS/FEMA, DHS Countering Weapons of Mass Destruction Office, and other DHS components as appropriate, for compliance with purposes and requirements of the priority investment area. Proposed investments will be reviewed for effectiveness using the criteria set forth in this NOFO.

All other proposed investments not associated with a required investment justification will undergo a Federal review by DHS/FEMA to verify compliance with all administrative and eligibility criteria identified in the NOFO.

Review and Selection Process (OPSG)
Applications will be reviewed by the SAA and USBP for completeness and adherence to programmatic guidelines and evaluated for anticipated feasibility, need, and impact of the

Operations Orders. For more information on Operations Orders and other requirements of OPSG, see the Preparedness Grants Manual.

DHS/FEMA will verify compliance with all administrative and eligibility criteria identified in the NOFO and required submission of Operations Orders and Inventory of Operations Orders by the established due dates. DHS/FEMA and USBP will use the results of both the risk analysis and the Federal review by DHS/FEMA to make recommendations for funding to the Secretary of Homeland Security.

FY 2020 OPSG funds will be allocated competitively based on risk-based prioritization using the OPSG Risk Assessment described above. Final funding allocations are determined by the Secretary, who may consider information and input from various law enforcement offices or subject-matter experts within the Department. Factors considered include, but are not limited to, threat, vulnerability, miles of the border, and other border-specific law enforcement intelligence, as well as the feasibility of FY 2020 Operations Orders to designated localities within border states and territories.

b. Financial Integrity Criteria

Prior to making a Federal award, DHS/FEMA is required by 31 U.S.C. § 3321 note, 41 U.S.C. § 2313, and 2 C.F.R. § 200.205 to review information available through any OMB-designated repositories of government-wide eligibility qualification or financial integrity information. Application evaluation criteria may include the following risk-based considerations of the applicant:

- Financial stability;
- Quality of management systems and ability to meet management standards;
- History of performance in managing Federal awards;
- Reports and findings from audits; and
- Ability to effectively implement statutory, regulatory, or other requirements.

c. Supplemental Financial Integrity Review

Prior to making a Federal award where the anticipated Federal share of a Federal award will be greater than the simplified acquisition threshold, currently $250,000 (*see* Section 805 of the National Defense Authorization Act for Fiscal Year 2008, Pub. L. No. 115-91, OMB Memorandum M-18-18 at https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-18.pdf; *see also* FEMA GPD Information Bulletin No. 434, Increases and Changes to the Micro-Purchase and Simplified Acquisition Thresholds):

- DHS/FEMA is required to review and consider any information about the applicant 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) and is also accessible through the SAM website.
- An applicant, at its option, may review information in FAPIIS and comment on any information about itself that a Federal awarding agency previously entered.
- DHS/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. § 200.205.

F. Federal Award Administration Information

1. Notice of Award

See the Preparedness Grants Manual for information on Notice of Award.

2. SHSP and UASI Pass-Through Requirements

Awards made to the SAA for HSGP carry additional pass-through requirements. Pass-through is defined as an obligation on the part of the SAA to make funds available to local units of government, combinations of local units, tribal governments, or other specific groups or organizations. Four requirements must be met to pass-through grant funds:

- The SAA must make a firm written commitment to passing through grant funds to subrecipients;
- The SAA's commitment must be unconditional (i.e., no contingencies for the availability of SAA 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.

Timing and Amount

The SAA must pass-through at least 80 percent of the funds awarded under the SHSP and UASI to local or tribal units of government within 45 calendar days of receipt of the funds. "Receipt of the funds" occurs either when the SAA accepts the award or 15 calendar days after the SAA receives notice of the award, whichever is earlier.

SAAs are sent notification of HSGP awards via the GPD's ND Grants system. If an SAA 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 SAA accepted the award. Should an SAA not accept the HSGP 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 SAA via the ND Grants system.

It is important to note that the PoP start date does not directly affect the start of the 45-calendar days pass-through period. For example, an SAA may receive notice of the HSGP award on August 20, 2020, while the PoP dates for that award are September 1, 2020, through August 31, 2022. In this example, the 45-day pass-through period will begin on the date the SAA accepts the HSGP award or September 4, 2020 (15 calendar days after the SAA was notified of the award), whichever date occurs first. The PoP start date of September 1, 2020 would not affect the timing of meeting the 45-calendar day pass-through requirement.

Other SHSP and UASI Pass-Through Requirements

The signatory authority of the SAA 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. The pass-through requirement does not apply to SHSP awards made to the District of Columbia, Guam, American Samoa, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands. The Commonwealth of Puerto Rico is required to comply with the pass-through requirement, and its SAA must also obligate at least 80 percent of the funds to local units of government within 45 calendar days of receipt of the funds.

Under SHSP, the SAA may retain more than 20 percent of funding for expenditures made by the state on behalf of the local unit(s) of government. This may occur only with the written consent of the local unit of government, specifying the amount of funds to be retained and the intended use of funds. States shall review their written consent agreements yearly and ensure that they are still valid. If a written consent agreement is already in place from previous fiscal years, DHS/FEMA will continue to recognize it for FY 2020, unless the written consent review indicates the local government is no longer in agreement. If modifications to the existing agreement are necessary, the SAA should contact their assigned FEMA HQ Program Analyst.

Additional OPSG Requirements
The recipient is prohibited from obligating or expending funds provided through this award until each unique and specific county-level or equivalent Operational Order/Fragmentary Operations Order budget has been reviewed and approved through an official electronic mail notice issued by DHS/FEMA removing this special programmatic condition.

3. **Administrative and National Policy Requirements**
   See the Preparedness Grants Manual for information on Administrative and National Policy requirements.

4. **Reporting**
   See the Preparedness Grants Manual for information on reporting requirements, including federal financial reporting requirements, programmatic performance reporting requirements, and closeout reporting requirements.

   Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Process
   See the Preparedness Grants Manual for information on the THIRA and SPR process.

   Supplemental Information Reporting Systems
   In addition to ND Grants, the following information systems are used for the submission of required reports:

   Grant Reporting Tool (GRT)
   Information on the GRT can be found in the Preparedness Grants Manual.

   Unified Reporting Tool (URT)
   See the Preparedness Grants Manual for information on the URT.

   Closeout Reporting Requirements
   See the Preparedness Grants Manual for information on closeout reporting requirements.

   Disclosing Information per 2 C.F.R. § 180.335
   See the Preparedness Grants Manual for information on disclosing information.

5. **Monitoring**
   Per 2 C.F.R. § 200.336, DHS/FEMA through its authorized representatives, has the right, at all reasonable times, to make site visits to review project accomplishments and management control

systems to review project accomplishments and to provide any required technical assistance. During site visits, DHS/FEMA will review grant recipients' files related to the grant award. As part of any monitoring and program evaluation activities, grant recipients must permit DHS/FEMA, 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/FEMA requests for information relating to the grant program**.** See the Preparedness Grants Manual for additional information on monitoring.

G. DHS/FEMA Awarding Agency Contact Information

1. Contact and Resource Information

Centralized Scheduling and Information Desk (CSID)
CSID is a non-emergency comprehensive management and information resource developed by DHS/FEMA for grant stakeholders. CSID provides general information on all DHS/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.gov, Monday through Friday, 9:00 a.m. – 5:00 p.m. ET.

GPD Grant Operations Division
GPD's Grant Operations Division Business Office provides support regarding financial matters and budgetary, technical assistance. Additional guidance and information can be obtained by contacting the FEMA Call Center at 866-927-5646 or via e-mail to ASK-GMD@fema.gov.

FEMA Regional Offices
FEMA Regional Offices may also provide fiscal support, including pre- and post-award administration and technical assistance such as conducting cash analysis, financial monitoring, and audit resolution for the grant programs included in this solicitation. GPD will provide programmatic support and technical assistance. FEMA Regional Office contact information is available here.

GPD Environmental Planning and Historic Preservation (EHP)
The DHS/FEMA GPD EHP Team provides guidance and information about the EHP review process to recipients and subrecipients. All inquiries and communications about GPD projects or the EHP review process, including the submittal of EHP review materials, should be sent to gpdehpinfo@fema.dhs.gov. EHP Technical Assistance, including the EHP Screening Form, can be found online at https://www.fema.gov/media-library/assets/documents/90195.

2. Systems Information

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.

Non-Disaster (ND) Grants
For technical assistance with the ND Grants system, please contact the ND Grants Helpdesk at

ndgrants@fema.gov or (800) 865-4076, Monday through Friday, 9:00 a.m. – 5:00 p.m. ET.

Payment and Reporting System (PARS)
DHS/FEMA uses the Payment and Reporting System (PARS) for financial reporting, invoicing and tracking payments. DHS/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 119A, Direct Deposit Form.

H. Additional Information

GPD has developed the Preparedness Grants Manual to guide applicants and recipients of grant funding on how to manage their grants and other resources. Recipients seeking guidance on policies and procedures for managing preparedness grants should reference the Manual for further information. Examples of information contained in the Preparedness Grants Manual include:

- Conflicts of Interest in the Administration of Federal Awards and Subawards;
- Extensions;
- Monitoring;
- Procurement Integrity; and
- Other Post-Award Requirements.

In response to recent disasters, FEMA has introduced a new lifelines construct, in order to enable the continuous operation of government functions and critical business essential to human health, safety, or economic security during and after a disaster. To learn more about lifelines, please refer to the Preparedness Grants Manual, or visit http://www.fema.gov/national-planning-frameworks.

Additionally, recipients can access the DHS Strategic Framework for Countering Terrorism and Targeted Violence which explains how the department will use the tools and expertise that have protected and strengthened the country from foreign terrorist organizations to address the evolving challenges of today.

AGENDA ITEM #4B

FFY 2020 NEVADA HOMELAND SECURITY GRANT PROGRAM (HSGP) BULLETIN

February 27, 2020

DELIVERABLES AND MEETING TIMELINE

Meeting or Deliverable	Description of Meeting	Meeting or Deliverable Due Date	Meeting Time or Deliverable Due Time
Completion of the 2019 THIRA/SPR	THIRA/SPR data is captured and used to create a heatmap to identify gap changes in capability statewide - Used by the NCHS to establish HSGP priorities for the following year.	12/31/2019	**COMPLETE**
FFY 2020 HSGP NOFO Released	Release of the FFY 2020 HSGP NOFO indicated allotment of funding applied to SHSP and UASI funding streams - This is the money Nevada projects will compete for.	2/14/2020	**COMPLETE**
Release of FFY20 HSGP Project Proposal requirements for Nevada's Grant application.	FFY20 HSGP Project Proposal submission into ZOOM Grants	2/17/2020	**COMPLETE**
Nevada Resilience Advisory Committee (NRAC) Meeting #1	FFY20 HSGP project submission overview	2/19/2020	**COMPLETE**
Urban Area Working Group (UAWG) Meeting #1	FFY20 HSGP project review for UASI and UASI/SHSP split projects – ***UASI only and UASI/SHSP split project presenters MUST attend.***	2/27/2020	**COMPLETE**
Nevada Commission on Homeland Security (NCHS) Meeting #1	FFY20 Discussion of HSGP timeline and overview	3/3/2020	9:00 a.m. - 10:30 a.m.
Urban Area Working Group (UAWG) Meeting #2	FFY20 UASI Project Prioritizing	3/9/2020	9:00 a.m. - 3:00 p.m.
Nevada Resilience Advisory Committee (NRAC) Meeting #2	FFY20 HSGP project review for SHSP or SHSP/UASI projects - ***Project presenter(s) for SHSP-only and SHSP/UASI split project submissions MUST attend.***	3/11/2020	9:00 a.m. – 5:00 p.m.
Nevada Office of Cyber Defense Coordination (OCDC) Review	Review of FFY20 cybersecurity-specific project submissions, prioritization, and recommendation to the Co-Chairs of the NRAC	TBD	N/A
Statewide Interoperability Coordinator (SWIC) Review	Review of FFY20 communications-specific project submissions, prioritization, and recommendation to the Co-Chairs of the NRAC	TBD	N/A
Urban Area Working Group (UASI) Meeting #3	UAWG meeting tentative if needed	3/17/2020	9:00 a.m. – Noon
Nevada Commission on Homeland Security (NCHS) – Finance Committee Meeting	Review of FFY20 NRAC recommendations for SHSP-only and SHSP/UASI split funded HSGP projects and to hear informational only UAWG recommendations for UASI-only HSGP funding; ***Project presenter(s) with projects recommended for funding should attend.***	4/1/2020	1:00 p.m. – 3:00 p.m.
Nevada Resilience Advisory Committee (NRAC) Meeting	Monthly Scheduled Meeting	4/8/2020	9:00 a.m. – 4:00 p.m.
Nevada Commission on Homeland Security (NCHS) Meeting #2	Review and Approval of FFY20 NRAC and UAWG recommendations; ***Project presenter(s) with projects recommended for funding should attend.***	4/9/2020	9:00 a.m. – 10:30 a.m.
Final State Application due to FEMA DHS Due	**Submission by DEM/HS of the final 2020 HSGP Grant application to DHS for consideration of project funding**	**4/14/2020**	**To DHS by 1:00 P.M. PST**

CONTACT INFORMATION AND QUESTIONS

Contact Name	Position Title	Phone No.	Email Address
Sonja Williams	Grants and Project Analyst	775-687-0388	swilliams@dps.state.nv.us or DHSGrants@dps.state.nv.us
Samantha Hill-Cruz	Grants and Projects Supervisor	775-687-0445	shillcruz@dps.state.nv.us
Kelli Anderson	Emergency Management Programs Manager	EMAIL ONLY	kanderson@dps.state.nv.us

AGENDA ITEM #5

Steve Sisolak
Governor

Nevada Department of Public Safety
DEDICATION PRIDE SERVICE

George Togliatti
Director

Sheri Brueggemann
Deputy Director

Justin Luna
Chief

Division of Emergency Management
Homeland Security
2478 Fairview Drive
Carson City, Nevada 89701
Telephone (775) 687-0300 / Fax (775) 687-0322
DEM Website – http://dem.nv.gov

Memorandum

DATE: February 27, 2020

TO: The Honorable Steve Sisolak, Governor, State of Nevada

FROM: Justin Luna, Chief, DPS Division of Emergency Management

SUBJECT: Report on the adoption of the National Incident Management System (NIMS)

NRS 239C.310 calls for the adoption of a national system of emergency response and requires the DPS Division of Emergency Management (DEM) to provide a report to the Nevada Commission on Homeland Security (NCHS) on a quarterly basis. Specifically, this statute states that the state, political subdivisions, and tribal governments in the state shall "adopt any national system that is required as a condition to the receipt of money from the Federal Government by the United States Department of Homeland Security pursuant to federal law in preparation for, prevention of, detection of, mitigation of, response to and recovery from a domestic incident, including, without limitation, an act of terrorism."

Historically, NIMS implementation has taken many forms. Local, tribal, and state governments, as well as the private sector, have adopted NIMS based upon federal guidance. DEM has coordinated the development and submission of various planning efforts; and all jurisdictions receiving funding through the Homeland Security Grant Program and the Emergency Management Performance Grant Program are required to meet standards of NIMS in order to participate.

DEM recently created a working group of statewide partners to establish levels of NIMS consistency throughout the statewide program. The group performed a survey to get a baseline of NIMS awareness and level of proficiency in each jurisdiction. Survey results were used to establish standards based on jurisdiction population, grant funding, and agency structure. The standards will be used to address compliance in the areas of preparedness, communications, resource management, command and support, and management and maintenance.