



CYBERSECURITY GRANTS FOR INFRASTRUCTURE  
IMPROVEMENT AND DEVELOPMENT  
**EXECUTIVE SUMMARY – FOCUS AREA 1**

**MISSION:** Gather and distribute information from federal agencies issuing grant funding for cybersecurity improvements to ensure that all 54 state, local, tribal, and territorial governments (SLTT) are best prepared to apply for and receive grant funding.

**SYNOPSIS:** Combatting cyber-crime and improving cybersecurity infrastructure across all levels of government requires significant financial resources to procure commercial products, develop new intellectual property, and attract and retain a talented workforce. Therefore, the States of Wyoming and Louisiana endeavored to identify, collect, and organize available information for its partners on available federal grants to help SLTTs make investments in their cyber infrastructure.

The attached materials provide a list of available grants, in alphabetical order, with each grant’s individual requirements, links to more in-depth information, and known point(s) of contact. The Council of Governor’s Cybersecurity Working Group hopes these materials serve as one-source reference for SLTT leadership.

**AUTHORS:** This is a joint project created by the States of Wyoming and Louisiana, with support from Governors Homeland Security Offices, Cybersecurity Infrastructure and Security Agency (CISA), the Department of Defense (DoD), and Federal Emergency Management Agency (FEMA).

**SOURCES:**

- [Public Law 117-58](#), referred to as the “Infrastructure Investment and Jobs Act.”
- National Defense Authorization Act for Fiscal Year 2022, [Public Law 117-81](#)
- Federal Funds Information for States (FFIS) ([www.FFIS.org](http://www.FFIS.org))
- [www.Grants.gov](http://www.Grants.gov)



**CYBERSECURITY GRANTS FOR INFRASTRUCTURE  
IMPROVEMENT AND DEVELOPMENT  
TABLE OF CONTENTS – FOCUS AREA 1**

<b>TABLE OF CONTENTS</b>		<b>Page No.</b>
<b>1</b>	<b>Executive Summary</b>	<b>1</b>
<b>2</b>	<b>Annual and Existing Available Grants</b>	
	<i>Defense Community Infrastructure Pilot Program</i>	<b>3</b>
	<i>Digital Equity Capacity Grant Program</i>	<b>4</b>
	<i>Emergency Management Performance Grant</i>	<b>5</b>
	<i>Emergency Operations Center Grant Program</i>	<b>6</b>
	<i>Energy, Power, Control, and Networks (EPCN) Program Grants</i>	<b>7</b>
	<i>Future Scholars and STEM Workforce</i>	<b>8</b>
	<i>Mobile Health: Technology and Outcomes in Low- and Middle-Income Countries</i>	<b>9</b>
	<i>Natural Gas Distribution Infrastructure Safety and Modernization Grant</i>	<b>10</b>
	<i>Operation Stonegarden Grant</i>	<b>11</b>
	<i>Port Security Grant Program</i>	<b>12</b>
	<i>State Homeland Security Program</i>	<b>13</b>
	<i>University Nuclear Leadership Program – Scholarship and Fellowship Support</i>	<b>14</b>
	<i>Urban Area Security Initiative</i>	<b>15</b>
	<i>State and Local Cybersecurity Grant Program</i>	<b>16</b>
	<i>Historically Black Colleges and Universities - Undergraduate Program</i>	<b>18</b>
	<i>National Science Foundation</i>	
<b>4</b>	<b>Expected/Future Grants</b>	
	<i>Exchange Grant Program</i>	<b>19</b>
	<i>Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program</i>	<b>19</b>
	<i>Strengthening Mobility and Revolutionizing Transportation Grant Program</i>	<b>20</b>
	<i>United States – Israel Cybersecurity Cooperation Grant</i>	<b>21</b>
<b>5</b>	<b>Success Stories</b>	<b>22</b>



**CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
ANNUAL AND EXISTING AVAILABLE GRANTS**

<b>Title of Grant:</b>	<b>Digital Equity Capacity Grant Program</b>
<b>Issuing Agency</b>	National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce
<b>General Summary</b>	<p>The purpose of grant is to promote the achievement of digital equity, support digital inclusion activities such as digital literacy and awareness of, and the use of, measure to secure the online privacy of, and cybersecurity with response to any individual; it is also intended to support the availability and affordability of consumer devices and technical support for those devices.</p> <p>Eligible entities include state, political subdivisions, non-profits (excluding schools and that do provide services within the state), any community anchor institution, local educational agency (including adult education and literacy activities), public and multi-family housing authority, and partnerships of any of the eligible entities. Each application must include 3 parts: 1) Identification of the barrier to digital equity in the state; 2) Measurable objectives anticipated by the project, such as availability and affordability of consumer devices and the online accessibility and inclusivity of public resources and services; and 3) How the objectives impact economic and workforce goals, educational outcomes, health outcomes, delivery of other essential services, and civic and social engagement.</p>
<b>Period of Availability</b>	Initial Notice of Funding Opportunity: <a href="#">NTIA-DE-PLAN-2022</a> , released May 13, 2022 (this is a 5-year annual grant).
<b>Funding Amount</b>	NTIA will make up to \$53,400,000 available under the State Digital Equity Planning Grant Program for States. Funding amounts for States will be determined pursuant to a statutory formula. U.S. territories and possessions (other than Puerto Rico), Indian Tribes, Alaska Native entities, and Native Hawaiian organizations that submit Letters of Intent.
<b>Key Link(s)</b>	<b>Public Law 117-58, Section 60304</b>
<b>Requirements</b>	The governor of each must select an agency within its jurisdiction to administer the grant, as well as develop, implement, and oversee the plan. The administering entity for the state shall make the State Digital Equity Plan of the State available for public comment for a period of not less than 30 days before the date on which the State submits the application to the Assistant Secretary of the Department of Commerce.
<b>Fiscal Restrictions/Notes</b>	State shall expend the grant funds during the 1-year period beginning on the date on which the State is awarded the grant funds. There is also a competitive version of this Grant, with \$250,000,000 in available grant funds per year, <i>for 5 years</i> , with a 10% cost-share for the states. <i>See Section 60305 “Digital Equity Competitive Grant Program” in Public Law 117-58. Not further addressed herein as it focuses more on broadband establishment.</i>
<b>Point(s) of Contact</b>	Scott McNichol, NIST Grants Officer, Grants Management Division, National Institute of Standards and Technology 325 Broadway, Boulder, CO 80305 Phone: (303) 497-3444   Email: <a href="mailto:scott.menichol@nist.gov">scott.menichol@nist.gov</a>



**CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
ANNUAL AND EXISTING AVAILABLE GRANTS**

<b>Title of Grant:</b>	<b>Defense Community Infrastructure Pilot Program</b>
<b>Issuing Agency</b>	Department of Defense
<b>General Summary</b>	<p>Office of Local Defense Community Cooperation under the Defense Community Infrastructure Pilot Program to provide State and local governments to address deficiencies in community infrastructure supportive of a military installation. The purpose of this grant is to fund community infrastructure projects, which are transportation projects, community support facilities (e.g., schools, hospitals, police, fire, and emergency response), and utility infrastructure projects (e.g., water, waste-water, telecommunications, electric, gas, etc.) that are located off of a military installation, support a military installation, and are owned by a State or local government or not-for-profit, member-owned utility.</p> <p>Eligible community infrastructure projects are any complete and useable transportation project; community support facilities (e.g., school, hospital, police, fire, emergency response, or other community support facility); and utility infrastructure projects (e.g., water, waste-water, telecommunications, electric, gas, or other utility infrastructure (with necessary cyber safeguards)) that are located near a military installation, support a military installation, are owned by a state or local government or a not-for-profit, member-owned utility service; enhance military value at a military installation, military installation resilience or military family life; are endorsed by the local installation commander representing the installation benefitting from the proposed project; and are construction ready.</p>
<b>Period of Availability</b>	Project dependent.
<b>Funding Amount</b>	\$90 Million – this is an annual grant.
<b>Key Link(s)</b>	Notice of Funding Opportunity Found through: <a href="https://oldcc.gov/defense-community-infrastructure-program-dcip#block1">https://oldcc.gov/defense-community-infrastructure-program-dcip#block1</a>
<b>Requirements</b>	Future Grant Deadlines Not Yet Available.
<b>Fiscal Restrictions/Notes</b>	Funding ceiling per award is \$20 Million; minimum award is \$250,000.00
<b>Point(s) of Contact</b>	Adam Wright, Office of Local Defense Community Cooperation, 2231 Crystal Drive, Suite 520, Arlington, VA 22202–3711. Office: (703) 697–2088 or (571) 721-9861. Email: adam.g.wright8.civ@mail.mil.



**CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
ANNUAL AND EXISTING AVAILABLE GRANTS**

<b>Title of Grant:</b>	<b>Emergency Management Performance Grant Program</b>
<b>Issuing Agency</b>	Federal Emergency Management Agency
<b>Eligible Entity</b>	State or Territorial Governments – State Administrative Agency or State’s Emergency Management Agency
<b>General Summary</b>	<p>This grant is not specific to cyber-related issues. This grant is designed to help SLTT support the National Preparedness Goal of a secure and resilient nation, through addressing the following objectives: 1) closing capability gaps that are identified in the state or territory’s most recent Stakeholder Preparedness Review (SPR); and 2) building or sustaining those capabilities that are identified as high priority through the Threat and Hazard Identification and Risk Assessment (THIRA)/SPR process and other relevant information sources.</p> <p>Applicants are strongly encouraged to focus their application on priorities set by the <a href="#">2022-2026 FEMA Strategic Plan</a>: Equity, Climate Resilience, and Readiness. While Climate Resilience is likely inapplicable to cyber, the goals of Equity and Readiness are applicable to cybersecurity. With naming “equity” as a foundation of emergency management, FEMA is looking for specific plans to serve each applicant’s under-resourced communities. An example of FEMA’s equity goal is partnering with Historically Black Colleges and Universities to create hiring pipelines for professionals in the emergency management fields. With cyber becoming an increasingly important element of emergency management, especially with the potential for cyber events to inflict kinetic consequences, establishing training and recruiting programs in cyber could present an opportunity to increase both the size and diversity of the cyber workforce in a state that promotes emergency management.</p> <p>With its readiness goal, FEMA seeks to expand its approach to agency readiness and reexamine its capabilities gaps. Identifying cyber risks inherent to emergency management, patching those risks, and developing alternative solutions to cyber-hazard scenarios increases emergency management readiness. With an additional focus on equity that builds a workforce focused on the cross-sections of cyber and emergency planning, the readiness goal of increasing opportunities and capabilities within the emergency management field is contemporaneously promoted.</p>
<b>Period of Availability</b>	October 1, 2021-September 30, 2024
<b>Funding Amount</b>	\$405,100,000.00 – Application deadline for FY passed on June 13, 2022
<b>Key Link(s)</b>	Department of Homeland Security Appropriations Act, 2022; Disaster Relief Supplemental Appropriations Act, 2022 <a href="https://www.fema.gov/grants/preparedness/emergency-management-performance/fy-22-nofo">https://www.fema.gov/grants/preparedness/emergency-management-performance/fy-22-nofo</a>
<b>Requirements</b>	All EMPG Program applicants are required to develop and submit a Work Plan as described in the “EMPG Program Work Plan” section of <a href="#">Appendix H of the Preparedness Grants Manual</a> . Recipients of this grant are required to implement the National Incident Management System (NIMS) and applications require final approval from the FEMA Regional Administrator.
<b>Fiscal Restrictions</b>	Funding opportunities divided by region.
<b>Point(s) of Contact</b>	State Emergency Operations Center/Agency



**CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
ANNUAL AND EXISTING AVAILABLE GRANTS**

<b>Title of Grant:</b>	<b>Emergency Operations Center Grant Program</b>
<b>Issuing Agency</b>	Federal Emergency Management Agency and Department of Homeland Security (together)
<b>Eligible Entity</b>	Only State Administrative Agencies (SAAs) (on behalf of state and local units of government) and Tribal governments with identified projects in <a href="#">Appendix A</a> of this funding notice are eligible to apply.
<b>General Summary</b>	<p>The Emergency Operations Center (EOC) Grant Program The fiscal year (FY) 2022 Emergency Operations Center (EOC) Grant Program is intended to improve emergency management and preparedness capabilities by supporting flexible, sustainable, secure, strategically located, and fully interoperable EOCs with a focus on addressing identified deficiencies and needs. The 2022-2026 FEMA Strategic Plan outlines three bold, ambitious goals in order to position FEMA to address the increasing range and complexity of disasters, support the diversity of communities we serve, and complement the nation’s growing expectations of the emergency management community. The EOC Grant Program supports Goal 3: Promote and Sustain a Ready FEMA and a Prepared Nation.</p> <p>The FY 2022 EOC Grant Program will provide \$49,026,403 for equipping, upgrading or constructing the EOC projects included in Appendix A of this funding notice. Per the National Fire Protection Association, an EOC is defined as a “facility or capability from which direction and control is exercised in an emergency. This type of center or capability is designated to ensure that the capacity exists for leadership to direct and control operations from a centralized facility or capability in the event of an emergency.” “Construction,” as defined in this program, refers to building a new facility or any changes to the footprint of an existing facility, while “upgrading” refers only to internal improvements to an existing facility.</p>
<b>Period of Availability</b>	Grant for FY 22 – 3 year period of performance (hope to be renewed annually through DHS Appropriations Act
<b>Funding Amount</b>	\$49,026,403 (for FY22)
<b>Key Link(s)</b>	<a href="https://www.fema.gov/grants/preparedness/emergency-operations-center#nofos">https://www.fema.gov/grants/preparedness/emergency-operations-center#nofos</a>
<b>Requirements</b>	This grant is only available to State Administrative Agencies. SAMS.gov registered is required to apply
<b>Fiscal Restrictions/Notes</b>	<p>Period of performance is 3 years. Application deadlines for FY23 not yet available.</p> <p>The FY 2022 EOC Grant Program has a cost share requirement. All award recipients must provide a non-federal entity contribution supporting 25% of the total of all project costs. The non-federal entity contribution can be cash (hard match) or third-party in-kind (soft match), with the exception of construction activities, which must be a cash (hard) match. In-kind contributions are defined as third-party contributions per 2 C.F.R. § 200.306.</p>
<b>Point(s) of Contact</b>	State Emergency Operations Center/Agency



**CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
ANNUAL AND EXISTING AVAILABLE GRANTS**

<b>Title of Grant:</b>	<b>Energy, Power, Control, and Networks (EPCN) Program Grants</b>
<b>Issuing Agency</b>	National Science Foundation, PD-18-7607
<b>Eligible Entities</b>	Institutions of Higher Education (IHEs) - Two- and four-year IHEs (including community colleges) accredited in, and having a campus located in the US, acting on behalf of their faculty members. Non-profit, non-academic organizations: Independent museums, observatories, research labs, professional societies, and U.S. organizations with educational or research activities.
<b>General Summary</b>	This is a research grant intended to encourage research on emerging technologies and applications including energy, transportation, robotics, and biomedical devices & systems. It is available to institutions of higher education and non-profit, non-academic institutions.
<b>Period of Availability</b>	Upcoming FY23 application deadlines not yet available.
<b>Funding Amount</b>	\$32,400,000.00
<b>Key Link(s)</b>	<a href="#">Grant Information for FY22</a> and <a href="#">General Program Information</a>
<b>Requirements</b>	<p>The two primary mechanisms for submitting proposals to NSF are through solicitations or to core programs. Core programs are standing programs that accept unsolicited proposals across the range of engineering disciplines. Cyber Physical Systems (CPS) is one core program accepting grant applications for research. Core research areas of the CPS program include control, data analytics, and machine learning including real-time learning for control, autonomy, design, Internet of Things (IoT), networking, privacy, real-time systems, safety, security, and verification.</p> <p>All proposals must include the following as part of the Project Description: 1) A Research Description that describes the technical rationale and technical approach of the CPS research, including the challenges that drive the research problem and how the research integrates cyber and physical components; 2) An Evaluation/Experimentation Plan that describes how proposed concepts will be validated and outlines the metrics for success; 3) A Project Management and Collaboration Plan that summarizes how the project team is ideally suited to realize the project goals and how the team will ensure effective collaboration; and 4) A “Broader Impacts” section that describes how the research will be disseminated to a broad and diverse audience.</p>
<b>Fiscal Restrictions</b>	Small projects may request a total budget of up to \$500,000 for a period of up to 3 years. They are well suited to emerging new and innovative ideas that may have high impact on the field of CPS. There is no deadline for small projects. Medium projects may request a total budget ranging from \$500,001 to \$1,200,000 for a period of up to 3 years. They are well suited to multi-disciplinary projects that accomplish clear goals requiring integrated perspectives spanning the disciplines. There is no deadline for Medium Projects. Frontier projects must address clearly identified critical CPS challenges that cannot be achieved by a set of smaller projects. Furthermore, Frontier projects should also look to push the boundaries of CPS well beyond today's systems and capabilities. Funding may be requested for a total of \$1,200,001 to \$7,000,000 for a period of 4 to 5 years. Note that the Frontier projects have a specific deadline.
<b>Point(s) of Contact</b>	David Corman, Program Director, <a href="mailto:dcorman@nsf.gov">dcorman@nsf.gov</a> , (703) 292-8754, Linda Bushnell, Program Director, <a href="mailto:lbushnel@nsf.gov">lbushnel@nsf.gov</a> , (703) 292-8950, Sandip Roy, Program Director, <a href="mailto:saroy@nsf.gov">saroy@nsf.gov</a> , (703) 292-8950





**CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
ANNUAL AND EXISTING AVAILABLE GRANTS**

Title of Grant:	Future Scholars and Stem Workforce
Issuing Agency	U.S. Airforce - the Air Force Research Laboratory (AFRL) at Kirkland Air Force Base, New Mexico
Eligible Entities	<ul style="list-style-type: none"> <li>▪ Native American tribal organizations (other than Federally recognized tribal governments)</li> <li>▪ Public and State controlled institutions of higher education</li> <li>▪ Native American tribal governments (Federally recognized)</li> <li>▪ Nonprofits having a 501(c)(3) status with the IRS, other than institutions of higher education</li> <li>▪ State, county, city, special district, or township governments</li> <li>▪ Independent school districts</li> <li>▪ Private institutions of higher education</li> </ul>
General Summary	This is a workforce development grant designed to create STEM educational programs, which includes cyber-related studies. The grant is open to institutions of higher education, nonprofit institutions, nonprofit organizations, States, local governments, Indian tribes, consortia of such institutions or nonprofit institutions/organizations. University Affiliated Research Centers (UARC) are eligible to submit applications under this FOA unless precluded from doing so by their Department of Defense UARC contract.
Period of Availability	Closing date for applications is June 17, 2025
Funding Amount	\$50,000,000.00 – Awaiting further appropriations (not accepting applications currently).
Key Link(s)	<a href="https://www.grants.gov/web/grants/view-opportunity.html?oppId=327212">https://www.grants.gov/web/grants/view-opportunity.html?oppId=327212</a>
Requirements	<p>All applications must be submitted through SAMs.gov. Prior to applying through Grants.gov, Recipients are required to submit, via e-mail, a Letter of Intent to the designated Grants and Agreements Officer and Contracting Specialist. The Letter of Intent shall not exceed two (2) pages and at a minimum provide the following details:</p> <ul style="list-style-type: none"> <li>▪ Title of the proposed effort.</li> <li>▪ Description of the proposed effort, to include by not limited to:               <ul style="list-style-type: none"> <li>○ Summary of how the proposed effort meets the AFRL’s programs Goals and Objectives as stated in Section I - Funding Opportunity Description.</li> <li>○ Rationale for the proposed effort.</li> <li>○ Details of how the success of the proposed effort will be met and the Recipient’s capacities for success in the proposed effort.</li> </ul> </li> <li>▪ Proposed period of performance (identify both the base period and any options, if applicable).</li> <li>▪ Total proposed budget (identify both the base period and any options, if applicable).</li> <li>▪ Administrative/business contact (name, address, phone, email address).</li> </ul>
Fiscal Restrictions	The minimum award amount for a proposed effort will be \$25,000.00. The maximum award amount for a proposed effort will be \$5,000,000.00 per year for a five-year total of \$25,000,000.00. Applications for larger amounts may be considered based on funding availability.
Point(s) of Contact	Sara Telano, Contracting Officer, <a href="mailto:sara.telano@us.af.mil">sara.telano@us.af.mil</a> , Lauren Rice, Contracting Specialist, <a href="mailto:lauren.rice.3@us.af.mil">lauren.rice.3@us.af.mil</a> , Email Subject: FOA-20-AFRL/RVKE-0001 Questions





**CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
ANNUAL AND EXISTING AVAILABLE GRANTS**

<b>Title of Grant:</b>	<b>Mobile Health: Technology and Outcomes in Low- and Middle-Income Countries</b>
<b>Issuing Agency</b>	Department of Health and Human Services (several participating healthcare agencies)
<b>Eligible Entities</b>	The following are entities eligible for this grant: Public/State/Private Institutions of Higher Education; Nonprofits with or without 501(c)(3) IRS Status (Other than Institutions of Higher Education); For-Profit Organizations, including Small Businesses; State, City, County, Special District, and Local Governments; Indian/Native American Tribal Governments & organizations (Federally Recognized or not); Independent School Districts; Public Housing Authorities/Indian Housing Authorities; Faith-based or Community-based Organizations; and Foreign components.
<b>General Summary</b>	<p>The purpose of this grant is to encourage exploratory/developmental research applications that propose to study the development, validation, feasibility, and effectiveness of innovative mobile health (mHealth) interventions or tools specifically suited for low and middle-income countries (LMICs) that utilize new or emerging technology, platforms, systems, or analytics. The overall goal of the program is to catalyze innovation through multidisciplinary research that addresses global health problems, develop an evidence base for the use of mHealth technology to improve clinical and public health outcomes, and strengthen mHealth research capacity in LMICs.</p> <p>This FOA encourages research projects that study the development, feasibility, validation, and effectiveness of mHealth tools and/or interventions for the prevention, diagnosis, management, and treatment of specific health conditions or for disease agnostic/cross-cutting applications. Applicants are encouraged to propose research projects that have the potential to provide an understanding of principles underlying effective mHealth interventions or tools that are generalizable to the field. Research projects may include some mHealth technology development along with feasibility, acceptability, usability, validation, and effectiveness studies. User-centered and iterative design are highly encouraged, as is taking a systems science approach, during development stages. Applications should include rigorous study designs as possible.</p>
<b>Period of Availability</b>	Fiscal Years 2022-2026.
<b>Funding Amount</b>	\$250,000,000
<b>Key Link(s)</b>	<a href="https://grants.nih.gov/grants/guide/pa-files/PAR-21-303.html">https://grants.nih.gov/grants/guide/pa-files/PAR-21-303.html</a>
<b>Requirements</b>	Awards are made under the authorization of Sections 301 and 405 of the Public Health Service Act as amended (42 USC 241 and 284) and under Federal Regulations 42 CFR Part 52 and 45 CFR Part 75.
<b>Requirements</b>	This grant provides financial support for up to two years for technology development and sustainability studies. All applicants must address <a href="#">R21</a> and <a href="#">R33</a> phases, but does not require clinical trials. The proposed research should be divided into the R21 and R33 phases as appropriate, with the milestone driven R21 demonstrating initial feasibility of the mHealth intervention or tool followed by further validation, feasibility, and/or effectiveness studies in the R33 phase.
<b>Fiscal Restrictions</b>	FY23 Application Dates not yet available.
<b>Point(s) of Contact</b>	Brad Newsome, PhD, Telephone: 1-301-480-8389, Email: <a href="mailto:brad.newsome@nih.gov">brad.newsome@nih.gov</a>



**CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
ANNUAL AND EXISTING AVAILABLE GRANTS**

Title of Grant:	<b>Natural Gas Distribution Infrastructure Safety and Modernization Grant</b>
<b>Issuing Agency</b>	Department of Transportation - Pipeline and Hazardous Materials Safety Administration
<b>General Summary</b>	<p>DOT’s Pipeline and Hazardous Materials Safety Administration (PHMSA) protects people and the environment by advancing the safe transportation of energy and other hazardous materials that are essential to daily lives. PHMSA’s NGDISM grants will provide funding to municipality- or community-owned utilities (not including for-profit entities) to repair, rehabilitate, or replace their natural gas distribution pipeline system or portions thereof, or to acquire equipment needed to (a) reduce incidents and fatalities and (b) avoid economic losses. The goals of this program are to 1) improve the safe delivery of energy to often underserved communities, reducing incidents and fatalities, as well as methane leaks; 2) avoid economic losses caused by pipeline failures; 3) to protect our environment and reduce climate impacts by remediating aged and failing pipelines and pipe prone to leakage; and 4) create good-paying jobs.</p> <p>Evaluation criteria will include the following: 1) the risk profile of the existing pipeline system operated by the applicant, including the presence of pipe prone to leakage; and 2) the extent to which disadvantaged rural and urban communities benefit from the remediation. Eligible entities are municipality-owned and community-owned operating a natural gas system. For profit entities are NOT eligible for this grant.</p>
<b>Period of Availability</b>	Congress appropriated \$1 billion over five years to implement and administer the NGDISM Grant Program. The period of performance is 36 months from the date of award for each grant.
<b>Funding Amount</b>	FY 22: 196,000,000.00 / FY 23 Information not yet available.
<b>Key Link(s)</b>	<a href="#">Notice of Funding Opportunity No. 693JK322NF0018</a>
<b>Requirements</b>	Application deadlines for FY23 not yet available. Applicants must provide a Statement of Work (SOW) addressing the scope, schedule, and budget for the proposed project (see Section D). The SOW must also include: 1) a risk profile describing the condition of the current infrastructure for which funding is requested—and potential safety benefits; 2) a plan for creating good-paying jobs that provides economic impact, growth, and substantial benefits to disadvantaged rural or urban communities; and 3) the proposal’s capacity to provide a reduction in lifecycle greenhouse gas emissions and any other impacts that may be beneficial to the environment or public.
<b>Fiscal Restrictions/Notes</b>	Award ceiling per applicant is \$45,000,000.00
<b>Point(s) of Contact/Resources</b>	Shakira Mack, <a href="mailto:PHMSAPipelineBILGrant@dot.gov">PHMSAPipelineBILGrant@dot.gov</a>   202-366-7652



**CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
ANNUAL AND EXISTING AVAILABLE GRANTS**

<b>Title of Grant:</b>	<b>Operation Stonegarden (OPSG)</b>
<b>Issuing Agency</b>	Federal Emergency Management Agency and Department of Homeland Security
<b>General Summary</b>	<p>The OPSG Program is part of the Homeland Security Grant Program, along with the Urban Area Security Initiative Grant and State Homeland Security Program Grant. The OPSG grant 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. The OPSG Program provides funding to support joint efforts to secure the United States’ borders along routes of ingress from international borders to include travel corridors in states bordering Mexico and Canada, as well as states and territories with international water borders.</p> <p>OPSG Applications are required to address the national priority and core capabilities as defined in the Notice of Funding Opportunity. In 2022, the National Priorities were listed as “enhancing information and intelligence sharing and analysis” in coordination with the Department of Homeland Security. The core capabilities are intelligence and information sharing, which heavily suggests a cyber nexus for improving real time communications.</p> <p>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/FEMA consider 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/FEMA considers the expected impact and consequences of successful border events occurring in specific areas.</p>
<b>Period of Availability</b>	FY2023 Application Deadlines not yet available.
<b>Funding Amount</b>	FY 22 received \$90 million in appropriations
<b>Key Link(s)</b>	FY 2022 <a href="#">Notice of Funding Opportunity</a>
<b>Requirements</b>	<p>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. The State Administrative Agency is the eligible applicant with county-level (or equivalent) governments eligible to serve as the subrecipients. All applicants must have DUNs number and each applicant must complete an environmental assessment if the plan will have an impact to the environment. SLTT law enforcement agencies utilizing 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.</p>
<b>Fiscal Restrictions/Notes</b>	Annual Grant with 3-year period of performance.
<b>Point(s) of Contact/Resources</b>	Centralized Scheduling and Information Desk (CSID), (800) 368-6498, <a href="mailto:askcsid@fema.dhs.gov">askcsid@fema.dhs.gov</a>



**CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
ANNUAL AND EXISTING AVAILABLE GRANTS**

<b>Title of Grant:</b>	<b>Port Security Grant Program</b>
<b>Issuing Agency</b>	Department of Homeland Security and Federal Emergency Management Agency
<b>General Summary</b>	<p>This grant provides funding to port authorities, facility operators, and state, local, and territory agencies for activities associated with implementing Area Maritime Security Plans (AMSP), facility security plans, and other port-wide risk management efforts. This grant is part of a comprehensive set of measures authorized by Congress and implemented to help strengthen the nation’s critical infrastructure against risks associated with potential terrorist attacks. The PSGP provides funds to state, local, and private sector maritime partners to support increased port-wide risk management and protect critical surface transportation infrastructure from acts of terrorism, major disasters, and other emergencies.</p> <p>The two top-tier priorities for this grant are 1) Enhancing cybersecurity; and 2. Enhancing the protection of soft targets/crowded spaces. The following are second-tier priorities for recipients in creating a comprehensive approach to securing critical maritime transportation infrastructure: 1) Effective planning; 2) Training and awareness campaigns; 3) Equipment and capital projects; and 4) Exercises.</p> <p>Eligible applicants include but are not limited to port authorities, facility operators, and state and local government agencies. A facility operator owns, leases, or operates any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the United States. Examples of facility operators include, but are not limited to terminal operators, ferry systems, bar/harbor pilots, and merchant’s exchanges.</p>
<b>Period of Availability</b>	September 1, 2022 – August 31, 2025
<b>Funding Amount</b>	\$100,000,000.00, 3 year period of performance.
<b>Key Link(s)</b>	<a href="#">Notice of Funding Opportunity No. DHS-22-GPD-056-00-01</a>
<b>Requirements</b>	FY23 Application Deadlines not yet available.
<b>Fiscal Restrictions/Notes</b>	There is a cost-share element for both public and private ports. Public-Sector Cost Share, for recipients other than private, for-profit entities—must provide a non-federal entity contribution supporting 25% of the total of all project costs as submitted in the application and approved in the award. Private, for-profit PSGP award recipients must provide a non-federal entity contribution supporting 50% of the total of all project costs as submitted in the application and approved in the award.
<b>Point(s) of Contact/Resources</b>	Centralized Scheduling and Information Desk (CSID) by phone at (800) 368-6498 or by email at <a href="mailto:askcsid@fema.dhs.gov">askcsid@fema.dhs.gov</a> , Monday through Friday, 9 a.m. – 5 p.m. ET.



CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
ANNUAL AND EXISTING AVAILABLE GRANTS

Title of Grant:	State Homeland Security Program (SHSP)
Issuing Agency	Department of Homeland Security
General Summary	<p><a href="#">State Homeland Security Program</a> (SHSP) grants assist local, State and Tribal <b>preparedness</b> activities that address <i>high-priority</i> preparedness <b>gaps</b> across <b>core capabilities</b> where an association to <b>terrorism exists</b>. Core capabilities are those capabilities with <b>five (5) mission areas</b> – <b>Prevention, Protection, Response, Recovery and Mitigation</b> – necessary to:</p> <ul style="list-style-type: none"> <li>▪ Avoid, <b>prevent</b> or stop a <i>threatened</i> or <b>actual act of terrorism</b>, within the United States.</li> <li>▪ Secure and <b>protect</b> the homeland against acts of <b>terrorism</b> and <b>man-made</b> or <b>natural disasters</b></li> <li>▪ Through <b>emergency disaster</b> and <b>response efforts</b>, save lives, protect property and the environment, and meet basic <b>human needs</b> <i>after</i> incident.</li> <li>▪ Assist communities affected by an emergency or disaster event with <b>recovering</b> <i>effectively</i>.</li> <li>▪ <i>Lessen</i> the impacts of disasters by <i>reducing</i> the <b>loss of life and property</b></li> </ul> <p>All supported investments are based on <b>capability targets and gaps identified</b> in achieving those targets, <b>during</b> the <b>Threat + Hazard Identification + Risk Assessment</b> (THIRA) process, and assessed in the <i>State Preparedness Report</i> (SPR). NOTE: there is no requirement to fund cybersecurity; it is optional.</p>
Period of Availability	FY23 Application Deadlines not yet available. This is an annual grant, with a 3 year period of performance.
Funding Amount	Awaiting Notice of Funding Opportunity for FY 2023.
Key Link(s)	<a href="https://www.fema.gov/grants/preparedness/homeland-security">https://www.fema.gov/grants/preparedness/homeland-security</a>
Requirements	<p>Grants are awarded to the State. Funds are allocated to <b>local governmental units</b>. The prime entity must perform at least <b>51%</b> of the project. At least <b>80%</b> of the funds awarded under SHSP must be <b>obligated</b> to <b>local government units</b> within <b>45 days</b> of the acceptance of the grant award. At <i>least</i> <b>25%</b> of funds allocated under SHSP and UASI <i>must</i> be <b>dedicated</b> towards <b>law enforcement terrorism prevention activities</b> (LETPA). The <b>State Administrative Agent</b> (SAA) is the <i>only</i> entity eligible to <b>apply</b> for and <b>administer</b> HSGP program funds. All subrecipients of SHSP ECSLP funds are required to complete the National Cybersecurity Review (NCSR)</p>
Fiscal Restrictions/Notes	<p>SHSP applicants are required to submit an Investment Justification (IJ) for each of the following five National Priority Areas and their associated minimum spend requirements:</p> <p>1) Enhancing cybersecurity – 7.5 percent; 2) Enhancing the protection of soft targets/crowded places – 5 percent; 3) Enhancing information and intelligence sharing and cooperation with federal agencies, including DHS – 5 percent; 4) Combating domestic violent extremism – 7.5 percent; and 5) Addressing emerging threats (e.g., transnational criminal organizations, unmanned aircraft systems [UASs], weapons of mass destruction [WMDs], etc.) – 5 percent. FEMA will award SHSP funds based on risk as determined by FEMA’s relative risk methodology pursuant to the Homeland Security Act of 2002.</p>
Point(s) of Contact/Resources	<ul style="list-style-type: none"> <li>▪ The FY 2022 HSGP Key Link(s) will be located online at <a href="http://www.fema.gov/grants">www.fema.gov/grants</a> as well as <a href="http://www.grants.gov">www.grants.gov</a>.</li> <li>▪ The FEMA Preparedness Grants Manual is located online at <a href="http://www.fema.gov/grants">www.fema.gov/grants</a>.</li> <li>▪ For additional program-specific information, please contact the Centralized Scheduling and Information Desk (CSID) help line at (800) 368-6498 or <a href="mailto:AskCSID@fema.dhs.gov">AskCSID@fema.dhs.gov</a>. CSID hours of operation are from 9 a.m. to 5 p.m. ET, Monday through Friday. <ul style="list-style-type: none"> <li>▪ For support regarding financial grants management and budgetary technical assistance, applicants may contact the FEMA Award Administration Help Desk via e-mail at <a href="mailto:ASK-GMD@fema.dhs.gov">ASK-GMD@fema.dhs.gov</a>.</li> </ul> </li> </ul>



**CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
ANNUAL AND EXISTING AVAILABLE GRANTS**

<b>Title of Grant:</b>	<b>University Nuclear Leadership Program – Scholarship and Fellowship Support</b>
<b>Issuing Agency</b>	Department of Energy
<b>General Summary</b>	This program awards multiple cooperative agreements to accredited United States (U.S.) two- and four-year colleges and universities (Institutions of Higher Education (IHEs)) to receive and administer scholarship and fellowship funding—provided through the University Nuclear Leadership Program (UNLP) and as administered by the Department of Energy, Office of Nuclear Energy (DOE-NE)—on behalf of selected students attending these U.S. IHEs. Eligible areas of study: programs in science and engineering disciplines related to nuclear energy such as Nuclear Engineering, Mechanical Engineering, Electrical Engineering, Chemistry, Health Physics, Nuclear Materials Science, Radiochemistry, Applied Nuclear Physics, Nuclear Policy, Radiation Protection Technology, Nuclear Power Technology, Nuclear Maintenance Technology, Nuclear Engineering Technology, Computer Science, and Cybersecurity at U.S. IHEs.
<b>Period of Availability</b>	Closes October 14, 2030. U.S. IHEs awarded under this FOA will be recognized for up to 13 years. However, in no event will new scholarships/fellowships be awarded after year 10 of this FOA.
<b>Funding Amount</b>	\$50,000,000 – There is an award ceiling of \$3,000,000.00
<b>Key Link(s)</b>	Key Link(s): DE-FOA-0002265 <a href="https://www.grants.gov/web/grants/view-opportunity.html?oppId=329436">https://www.grants.gov/web/grants/view-opportunity.html?oppId=329436</a>
<b>Requirements</b>	A list of eligible universities: <a href="https://neup.inl.gov/SitePages/UNLP%20Approved%20Universities.aspx">https://neup.inl.gov/SitePages/UNLP%20Approved%20Universities.aspx</a> Applications must be submitted through <a href="http://www.neup.gov">www.neup.gov</a> . The administrative requirements for DOE grants and cooperative agreements are contained in 2 CFR 200, as amended by 2 CFR 910 (see <a href="http://www.eCFR.gov">http://www.eCFR.gov</a> ).
<b>Fiscal Restrictions/Notes</b>	Graduate Scholarships: maximum of up to \$161,000 total for three (3) contiguous years will be awarded per student. This equates to a maximum of \$52,000 per year, with an additional \$5,000 provided to offset the costs of a 10-week minimum internship required of all fellows.  Four-year College/University Undergraduate Scholarship Program to \$10,000. Two-year Trade School and Community College Scholarship Program for \$5,000
<b>Point(s) of Contact/Resources</b>	Name: Julie Jacobson, E-mail: <a href="mailto:Julie.Jacobson@inl.gov">Julie.Jacobson@inl.gov</a> , Telephone: 208-526-6760 Name: Andrew Ford, E-mail: <a href="mailto:fordaj@id.doe.gov">fordaj@id.doe.gov</a> , Telephone: 208-526-3059





CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
ANNUAL AND EXISTING AVAILABLE GRANTS

Title of Grant:	Urban Area Security Initiative (UASI)
Issuing Agency	Department of Energy - DE-FOA-0002503   National Energy Technology Laboratory
General Summary	<p>Contributes to <i>high-threat, high-density urban areas</i> in their efforts to build and <i>sustain</i> the <b>capabilities</b> essential to <b>prevent, protect</b> against, <b>mitigate, respond</b> to, and <b>recover</b> from acts of <b>terrorism</b>. This grant is part of the Homeland Security Grant Program. In evaluating applications, the applicants must demonstrate a nexus to achieving target capabilities related to preventing, preparing for, protecting against, and responding to acts of terrorism. Certain core capabilities and national priorities include cybersecurity, enhancing election security, vulnerability assessments, and enhancing information and intelligence sharing and analysis.</p> <p>In its application, each high-risk urban area, through the state, must include a separate IJ for each of the four National Priority Areas with minimum spend requirements. All projects related to the minimum spend for the National Priority Area must be included in the IJ. For the National Priority Areas that have a minimum spend percentage requirement, the funding level in each of those National Priority Area investments must equal or exceed the percentage for that respective National Priority Area, calculated as a percentage of the urban area’s UASI allocation in the table below. The funding levels across all six National Priority Areas must equal or exceed 30 percent of the total UASI allocation.</p> <p>To determine areas that represent <i>highest risk</i> – and consistent with the <a href="#">Implementing Recommendations of the 9/11 Commission Act of 2007</a> (9/11 Act) – FEMA conducts <b>risk assessments</b> for the <b>100 most populous metropolitan areas</b> prior to making UASI grant awards.</p>
Period of Availability	September 1, 2022 - August 31, 2025. FY23 Notice of Funding Opportunity and applicable deadlines not yet available.
Funding Amount	\$615,000,000.00 – funding assigned to specifically designated cities.
Key Link(s)	<a href="https://www.fema.gov/grants/preparedness/homeland-security">https://www.fema.gov/grants/preparedness/homeland-security</a>
Requirements	<ul style="list-style-type: none"> <li>▪ Urban areas representing up to <b>85%</b> of the nationwide risk are most likely to be funded.</li> <li>▪ At <i>least</i> <b>25%</b> of funds allocated under SHSP and UASI <i>must</i> be <b>dedicated</b> towards <b>law enforcement terrorism prevention activities</b> (LETPA).</li> <li>▪ Eligible activities include <b>planning, organization, equipment, training</b> and <b>exercise</b> needs of <i>high-threat, high-density urban areas</i>.</li> <li>▪ The <b>State Administrative Agent</b> (SAA) is the <i>only</i> entity eligible to apply to FEMA for UASI funds.</li> </ul>
Fiscal Restrictions/Notes	UASI applicants are required to submit an Investment Justification (IJ) for each of the following five National Priority Areas and their associated minimum spend requirements: 1) Enhancing cybersecurity – 7.5 percent; 2) Enhancing the protection of soft targets/crowded places – 5 percent; 3) Enhancing information and intelligence sharing and cooperation with federal agencies, including DHS – 5 percent; 4) Combating domestic violent extremism – 7.5 percent; and 5) Addressing emerging threats (e.g., transnational criminal organizations, unmanned aircraft systems [UASs], weapons of mass destruction [WMDs], etc.) – 5 percent. FEMA will award UASI funds based on risk.
Point(s) of Contact/Resources	Centralized Scheduling and Information Desk (CSID) help line at (800) 368-6498 or AskCSID@fema.dhs.gov.





## CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT ANNUAL AND EXISTING AVAILABLE GRANTS

<b>Title of Grant:</b>	<b>State and Local Cybersecurity Improvement Act Grant</b>
<b>Issuing Agency</b>	Department of Homeland Security, through the Cybersecurity and Infrastructure Security Agency
<b>General Summary</b>	This grant is available to State and Tribal governments that apply to the Secretary of the Department of Homeland Security. Any awarded funds are required to be used to implement a “Cybersecurity Plan,” develop a Cybersecurity Plan, pay administrative expenses for that plan, and assist with activities that address imminent cybersecurity threats identified by DHS.
<b>Period of Availability</b>	Until expended (estimated FY22-25) – Notice of Funding Opportunities Released Annually.
<b>Funding Amount</b>	\$1,000,000,000.00
<b>Key Link(s)</b>	<a href="#">Public Law 117-58, Section 70611 “State and Local Cybersecurity Improvement Act”</a>
<b>Requirements</b>	<ul style="list-style-type: none"> <li>▪ Only 5% of the total grant funds may be used for administration of the plan’s implementation and oversight.</li> <li>▪ 80% of the funds must reach State and Local infrastructure with 25% of funds also impacting rural areas.</li> <li>▪ DHS requires the State or Tribal government to develop and implement a Cybersecurity Plan and include the plan with its application for the grant.</li> <li>▪ Qualifying Cybersecurity Plans must incorporate, to the extent practicable, any existing plans protecting against cybersecurity risks/threats in consultation with local governments and describe how it will meet <b>16 elements</b>:             <ol style="list-style-type: none"> <li>1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by the State and its local governments, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology;</li> <li>2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts;</li> <li>3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts against cybersecurity risks and cybersecurity threats;</li> <li>4. Implement a process of continuous vulnerability assessments and threat mitigation practices prioritized by degree of risk on information systems, applications, and user accounts;</li> <li>5. Ensure that the State and its local governments adopt and use best practices and methodologies to enhance cybersecurity, such as NIST, supply chain risk management, and knowledge bases;</li> <li>6. Promote the delivery of safe, recognizable, and trustworthy online services, including through the use of the .gov internet domain;</li> <li>7. Ensure continuity of operations of the State and its local governments, in the event of a cybersecurity incident, including cybersecurity exercises to practice incident response;</li> <li>8. Use the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity to identify and mitigate any gaps in the cybersecurity workforces of the State and its local governments, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training;</li> <li>9. Ensure continuity of communications and data networks in the event of an incident involving those communications or data networks;</li> </ol> </li> </ul>



## CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT ANNUAL AND EXISTING AVAILABLE GRANTS

10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems;
11. Enhance capabilities to share cyber threat indicators and related information between the State, local governments, and DHS;
12. Leverage cybersecurity services offered by DHS;
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives;
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats between State and local governments.
15. Ensure adequate access to, and participation in, the services and programs by Rural areas;
16. Distribute funds, items, services, capabilities, or activities to local governments and rural areas as follows: not less than 80% of the funds awarded available to local governments and 25% of total value of the grant must reach rural areas (which may include local governments).

### Additional Requirements:

- Assess the capabilities of the State based on the requirements of the Grant;
- Describe, as appropriate and to the extent practicable, the individual responsibilities of the State and local governments;
- Outline, to the extent practicable, the necessary resources and a timeline for implementing the plan; and
- Describe the metrics the State will use to measure progress towards implementing the plan; and reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by the State and the local governments.

### Fiscal Restrictions/Notes

- Each State/Territory was assigned a set, baseline amount by DHS with additional funding available based on each one's respective populations. The funding is available over 4 years, with \$200 Million available in FY 22, \$400 Million available in FY 23, \$300 Million available in FY 24, and \$100 Million available in FY 25.
- Cost Shares change based upon single applicant status v. multi-entity applications:
  - For single States/Territories:
    - FY 22: 90% Fed and 10% State
    - FY 23: 80% Fed and 20% State
    - FY 24: 70% Fed and 30% State
    - FY 25: 60% Fed and 40% State
  - For Multi-Groups:
    - FY 22: 100% Fed and 0% State
    - FY 23: 90% Fed and 10% State
    - FY 24: 80% Fed and 20% State
    - FY 25: 70% Fed and 30% State

### Point(s) of Contact

[central@cisa.gov](mailto:central@cisa.gov), 888-282-0870



CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
ANNUAL AND EXISTING AVAILABLE GRANTS

Title of Grant:	HBCU – Undergraduate Program
Issuing Agency	National Science Foundation
General Summary	<p>BCU-UP provides awards to strengthen STEM undergraduate education and research at HBCUs, through:</p> <ul style="list-style-type: none"> <li>• <b>Targeted Infusion Projects (TIP)</b>, which provide support to achieve a short-term, well-defined goal for improving the quality of undergraduate STEM education at HBCUs.</li> <li>• <b>Broadening Participation Research (BPR)</b> in STEM Education projects, which provide support for research that seeks to create and study new theory-driven models and innovations related to the participation and success of underrepresented groups in STEM undergraduate education.</li> <li>• <b>Research Initiation Awards (RIA)</b>, which provide support for STEM faculty with no prior or recent research funding to pursue research at the home institution, a NSF-funded research center, a research intensive institution, or a national laboratory.</li> <li>• <b>Implementation Projects (IMP)</b>, which provide support to design, implement, study, and assess comprehensive institutional efforts for increasing the number of students receiving undergraduate degrees in STEM and enhancing the quality of their preparation by strengthening STEM education and research. Within this track, Achieving Competitive Excellence (ACE) Implementation Projects are intended for HBCUs with exemplary achievements and established institutionalized foundations from previous Implementation Project grants.</li> <li>• <b>Broadening Participation Research Centers (BPRC)</b>, which provide support to conduct broadening participation research at institutions that have held three rounds of Implementation or ACE Implementation Projects and with demonstrated capability to conduct broadening participation research. Broadening Participation Research Centers are expected to represent the collective intelligence of HBCU STEM higher education, and serve as national hubs for the rigorous study and broad dissemination of the critical pedagogies and culturally sensitive interventions that contribute to the success of HBCUs in educating African American STEM undergraduates. Centers are expected to conduct research on STEM education and broadening participation in STEM; perform outreach to HBCUs in order to build capacity for conducting this type of research; and work to disseminate promising broadening participation research in order to enhance STEM education and research outcomes for African American undergraduates across the country.</li> <li>• Other Funding Opportunities include Early-Concept Grants for Exploratory Research (EAGER), Rapid Response Research (RAPID), conference, and planning grants.</li> </ul>
Period of Availability	FY23 through FY24
Funding Amount	\$55,000,000.00 in total program funding; Award ceiling at \$9,000,000.00.
Key Link(s)	<a href="#">National Science Foundation Information Page</a>
Requirements	Letters of Intent are required and due July 25, 2023; Application deadlines depend on type of funds being sought.
Fiscal Restrictions/Notes	Eligible entities are: Historically Black Colleges and Universities (HBCUs) that are accredited and offer undergraduate educational degree programs in science, technology, engineering and mathematics (STEM).
Point(s) of Contact	Carleitta L. Paige-Anderson, E-mail: <a href="mailto:cpaigean@nsf.gov">cpaigean@nsf.gov</a> , Phone: (703) 292-2816



**CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
EXPECTED/FUTURE GRANTS**

<b>Title of Grant:</b>	<b>Exchange Grant Program</b>
<b>Issuing Agency</b>	Department of Health and Human Services
<b>General Summary</b>	This grant is for American Health Benefits Exchanges that are established under Section 1311(b) of the Patient Protection and Affordable Care Act (42 U.S.C. 18031(b)) to modernize technology or update systems for the exchanges. This grant is similar to previous Exchange Grants that subsidized (through federal funding) the establishment of ACA exchanges within the states and federal qualified healthcare centers. The new Exchange Grant Program is found in the American Rescue Act of 2021.
<b>Period of Availability</b>	Unknown – FY 22 funding not released.
<b>Funding Amount</b>	\$20,000,000.00
<b>Key Link(s)</b>	<a href="https://www.congress.gov/117/plaws/publ2/PLAW-117publ2.pdf">https://www.congress.gov/117/plaws/publ2/PLAW-117publ2.pdf</a>
<b>Requirements</b>	Not yet released.
<b>Fiscal Restrictions/Notes</b>	Not yet released.
<b>Point(s) of Contact</b>	Not yet released.

<b>Title of Grant:</b>	<b>Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program</b>
<b>Issuing Agency</b>	Department of Energy
<b>General Summary</b>	This competitively awarded grant is intended to assist rural and municipal utility providers with deploying advanced cybersecurity technologies for electric utility systems and increase their participation of eligible entities in cybersecurity threat information sharing programs. All applications submitted for the grant will be exempt from Freedom of Information Act Requirements. The Department of Energy posted Requests for Information for reply by December 2022. However, FY23 information is not yet released.
<b>Period of Availability</b>	Fiscal Years 2022-2026
<b>Funding Amount</b>	\$250,000,000
<b>Key Link(s)</b>	<b>Public Law 117-58, Section 40124, <a href="#">Department of Energy Website</a></b>
<b>Requirements</b>	Eligible entities for the grant: rural electric cooperatives, public or privately-owned (or quasi-public) utilities, a not-for-profit entity that is in a partnership with no less than 6 entities that are either rural electric cooperatives or public or privately owned utilities (including any combination thereof), or an investor-owned electric utility that sells less than 4,000,000 megawatt hours of electricity per year. There is priority given to entities with limited cybersecurity resources that own assets critical to the reliability of the bulk power system; or owns defense critical electric infrastructure.
<b>Fiscal Restrictions/Notes</b>	The Notice of Funding Opportunity is not yet released. The grant requires that not less than 50 percent of the cost of a research, development, demonstration, or commercial application program or activity described in the grant application be provided by a non-federal source.
<b>Point(s) of Contact</b>	Not yet released.



**CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
EXPECTED/FUTURE GRANTS**

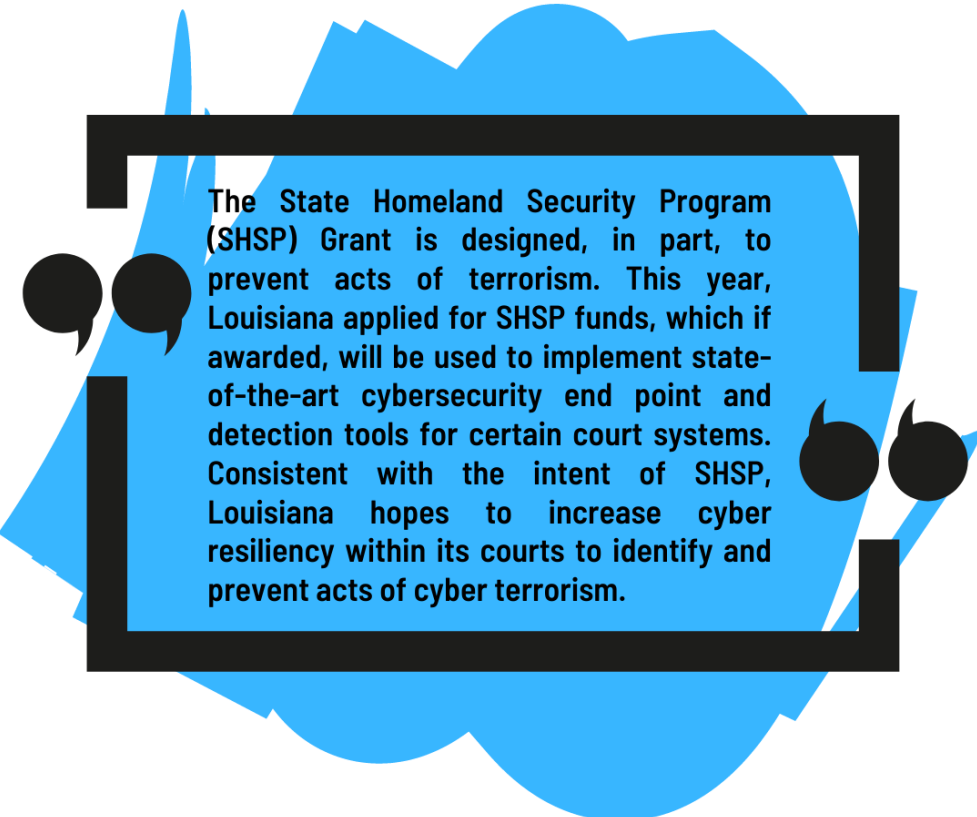
<b>Title of Grant:</b>	<b>Strengthening Mobility and Revolutionizing Transportation Grant Program</b>
<b>Issuing Agency</b>	Department of Homeland Security
<b>General Summary</b>	<p>This grant is available for information technology work and systems management (in addition to planning, revenue forecasting, property acquisition, and environmental reviews). Entities eligible to receive this grant are: SLTTs, a public transportation agency, a public tool authority, a metropolitan planning organization, or any of these two eligible entities working together. Referred to as a “SMART” Grant, it is intended to allow eligible entities to conduct demonstration projects focused on advanced smart city or community technologies to improve transportation efficiency and safety. This is a competitive grant program for city or community demonstration project that incorporate innovative transportation technologies or uses of data, including coordinated automation, connected vehicles, and intelligent sensor-based infrastructure. The Secretary is directed to consider geographic diversity and select projects across rural, midsized, and large communities.</p> <p>Application information for FY23 not yet available.</p>
<b>Period of Availability</b>	Fiscal Years 2022-2026.
<b>Funding Amount</b>	\$100,000,000.00 a year for 5 years – available for obligation during the first two fiscal years following appropriation.
<b>Key Link(s)</b>	<b>Public Law 117-58, Section 25005 – <a href="#">Fact Sheet</a> and <a href="#">Department of Transportation Website</a></b>
<b>Requirements</b>	<p>Each eligible entity must submit an application to the Secretary that identifies the following: 1) Whether the eligible entity has a public transportation system or other transit option open to efficiency improvements through integration; 2) Whether the eligible entity has a population density capable of utilized improved transportation programs; 3) Whether the eligible entity has continuity of leadership and functional capacity to execute the project; 4) Whether the eligible entity will participate in open data sharing with the public; 5) Whether the eligible entity can demonstrate likelihood of success, including through the technical and financial commitments from the public and private sectors.</p> <p>The applying entity must also show the extent to which the proposed project will use advanced data, technology, and applications to provide significant benefits to a local area, state, region and the extent to which the project will: 1) reduce congestion and transportation delays; 2) improve the safety and integration of different types transportation (bikes, walking paths); 3) improve access to jobs, education, health care, and other essential services; 4) connect or expand access for underserved or disadvantaged populations; 5) contribute to medium and long-term economic competitiveness; 6) improve the reliability of existing transportation facilities and systems; 7) promote connectivity between connected vehicles, roadway infrastructure, pedestrians, cyclists, and public transportation systems; 8) improve energy efficiency or reduce pollution; 9) incentivize private sector investments or partnerships, including by working with mobile and fixed telecommunication service providers, to the extent practicable; 10) increase resiliency of transportation program; and 11) improve emergency response.</p>
<b>Fiscal Restrictions/Notes</b>	Grant funds cannot be used to purchase license plate readers, any traffic/parking enforcement activity, and reimburse any pre-award costs or application preparation costs.
<b>Point(s) of Contact</b>	Not yet released.



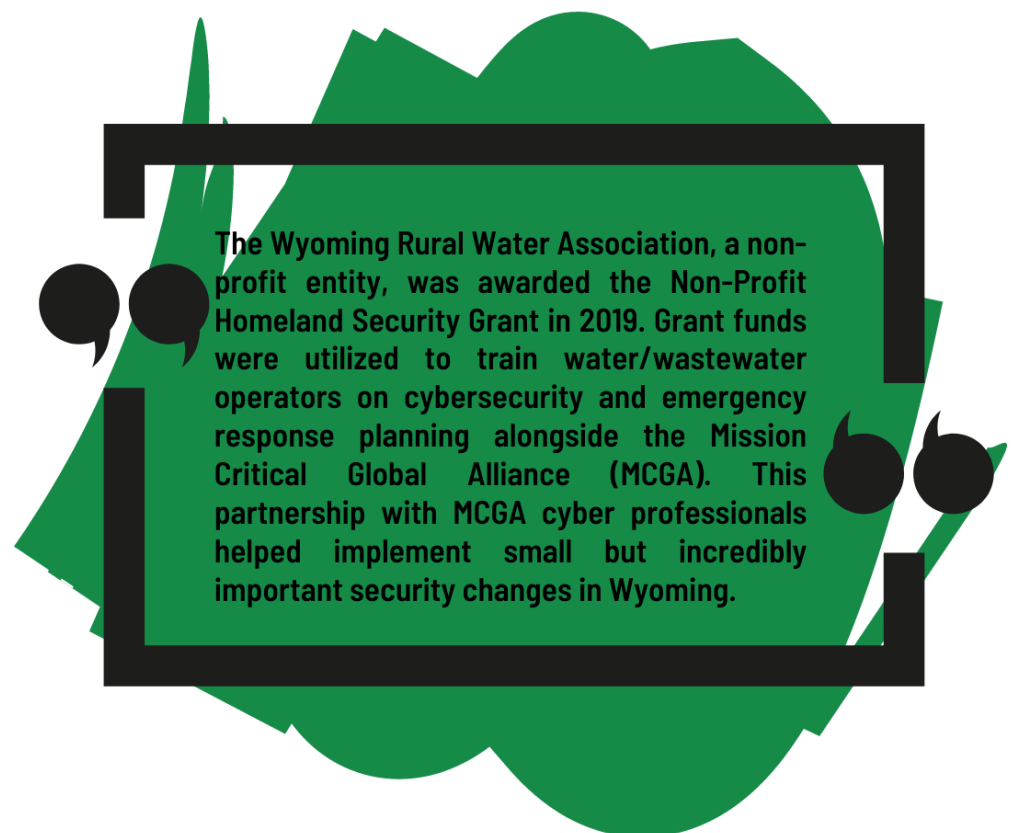
**CYBERSECURITY GRANTS FOR INFRASTRUCTURE IMPROVEMENT AND DEVELOPMENT  
EXPECTED/FUTURE GRANTS**

<b>Title of Grant:</b>	<b>United States – Israel Cybersecurity Cooperation Grant</b>
<b>Issuing Agency</b>	Department of Homeland Security
<b>General Summary</b>	This grant is for cybersecurity research and development and the demonstrated commercialization of cybersecurity technology. It is intended for joint ventures between U.S. entities (can be an educational institution, for-profit company, or non-profit company) and an Israeli entity (educational, for-profit, or non-profit) OR agencies of the U.S. and Israeli government.  Fiscal Year 2023 Information Not yet Available.
<b>Period of Availability</b>	Fiscal Years 2022-2026.
<b>Funding Amount</b>	\$6,000,000.00
<b>Key Link(s)</b>	<b>Public Law 117-81, Section 1551</b>
<b>Requirements</b>	Not yet released.
<b>Fiscal Restrictions/Notes</b>	Not yet released. The grant requires that no less than 50 percent of the cost of a research, development, demonstration, or commercial application program or activity described in the grant application be provided by a non-federal source.
<b>Point(s) of Contact</b>	Not yet released.

Many annual grants are designed to secure critical infrastructure, improve emergency operations, and prevent acts of terrorism. Although often earmarked for physical security or emergency supplies, flexible grant requirements may allow eligible entities to apply any awarded funds towards cybersecurity efforts to prevent acts of domestic terrorism and secure emergency communications. See examples below:



The State Homeland Security Program (SHSP) Grant is designed, in part, to prevent acts of terrorism. This year, Louisiana applied for SHSP funds, which if awarded, will be used to implement state-of-the-art cybersecurity end point and detection tools for certain court systems. Consistent with the intent of SHSP, Louisiana hopes to increase cyber resiliency within its courts to identify and prevent acts of cyber terrorism.



The Wyoming Rural Water Association, a non-profit entity, was awarded the Non-Profit Homeland Security Grant in 2019. Grant funds were utilized to train water/wastewater operators on cybersecurity and emergency response planning alongside the Mission Critical Global Alliance (MCGA). This partnership with MCGA cyber professionals helped implement small but incredibly important security changes in Wyoming.