Subject Specific Grant Guide

Grants to Support Cyber Security Projects

This guide identifies potential funding opportunities to support cyber security projects, including cyber security workforce development and addressing crime committed online. The opportunities chosen for inclusion in this guide are opportunities that are typically reoccurring and were released during 2023. Past funding opportunities that seemed relevant but presented no indication of being funded in the future were not included.

August 2024

Prepared by
The Ferguson Group

1901 Pennsylvania Ave. NW
Suite 700
Washington, DC 20006

202.331.8500

TheFergusonGroup.com

Table of Contents

U.S. Department of Commerce 1

Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Education and Workforce Development 1

U.S. Department of Defense 4

Future Scholars for Science, Technology, Engineering, and Mathematics (STEM) Workforce Development Programs 4

U.S. Department of Energy 7

Rural and Municipal Utility Advances Cybersecurity Grant and Technical Assistance Program 7

U.S. Department of Homeland Security 11

Homeland Security National Training Program 11

Port Security Grant Program 14

State Homeland Security Program 18

State and Local Cybersecurity Grant Program 23

Transit Security Grant Program 26

National Science Foundation 29

Energy, Power, Control, and Networks Program 29

Free Resources 32

FEDERAL
GRANT PROFILE

Department: U.S. Department of Commerce
Agency: National Institute of Standards and Technology

FY 2024 Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Education and Workforce Development

Grant Overview

This program is seeking applications from eligible applicants for activities to establish multistakeholder partnerships to develop cybersecurity career pathways that address local workforce needs. Eligible applicants are accredited institutions of higher education; non-profit organizations; for-profit organizations incorporated in the United States; state, local, territorial, and Indian tribal governments; foreign public entities; and foreign organizations.

Program History

	Total Funding	# of Awards
2016	$1 million	5

Key Information

Total Funding: Unspecified
Award Range: Up to $200,000
Match: 50 percent
Solicitation date: June 6, 2023
Proposal due: August 7, 2023

https://www.grants.gov/web/grants/view-opportunity.html?oppId=348550

Tips

- Regional alliances must include letters of commitments from participating organizations
- Diversity, Equity, Inclusion, and Accessibility are essential priorities to diversify the cybersecurity workforce and reach underserved and underrepresented communities
- A webinar for interested applicants will be held on June 13, 2023 at 1-2pm Eastern Time

Department: U.S. Department of Commerce
Agency: National Institute of Standards and Technology

FY 2024 Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Education and Workforce Development

Detailed Summary

The purpose of this program is to support activities to establish a multistakeholder partnerships to develop cybersecurity career pathways that address local workforce needs. Each application must include a plan to establish a multistakeholder education and workforce partnership that includes, at a minimum, one institution of higher education or nonprofit training organization, and one local employer or owner or operator of critical infrastructure or identify any such existing partnership. Participation from more than one of each of these types of organizations, as well as from one or more academic institutions in the Federal Cyber Scholarships for Service Program, the National Centers of Academic Excellence in Cybersecurity Program, or advanced technological education programs, as well as elementary and secondary schools, training and certification providers, economic development organizations, and other community organizations, is encouraged.

Successful projects will create the local conditions, such as infrastructure for education providers, employers, and others to develop the cybersecurity education capabilities, to create an ecosystem equipped to fill a critical skills gap for the economy.

Proposed projects must:

- Demonstrate how the activity aligns with the Department of Commerce Strategic Plan, meets the Effective Workforce Investment Criteria, and advances the Good Jobs Principles
- Prioritize diversity, equity, inclusion, and accessibility as an essential requirement in strategies intended to diversify the cybersecurity workforce and reach underserved and under-represented communities
- Ensure that that the partnership is employer-led, community-focused, learner-centered, standards-based, and outcomes-driven
- Describe planned initiatives that align to the goals and objectives of the National Initiative for Cybersecurity Education (NICE) Strategic Plan or help support the strategies of the NICE Implementation Plan
- Advance uses of the NICE Framework, including through demonstration of how the stakeholders intend to use the NICE Framework
- Identify the workforce needs of the local economy and assess such workforce in accordance with the NICE Framework, including ideas for how the multistakeholder organization would leverage the CyberSeek job heat map and career pathways

- Identify opportunities available and recruit employers to support paid internships, externships, apprenticeships, or cooperative education programs in conjunction with education and training providers in the local community
- Identify collaboration with one or more Center of Academic Excellence in Cybersecurity (CAE), Advanced Technological Education (ATE) programs, or Federal CyberCorps Scholarship for Service (SFS) institutions located in the region
- Define metrics that will be used to measure the success of program efforts.

Applicant Eligibility

Eligibility for the program is open to all nonfederal entities. Eligible applicants include accredited institutions of higher education; non-profit organizations; for-profit organizations incorporated in the United States; state, local, territorial, and Indian tribal governments; foreign public entities; and foreign organizations. Please note that individuals and unincorporated sole proprietors are not considered "non-Federal entities" and are not eligible to apply to this program. Although Federal entities are not eligible to receive funding under this program, they may participate as unfunded collaborators.

Applicants must also demonstrate through commitment letters that at least one of each of the following types of organizations is committed to being part of the proposed multistakeholder workforce partnership:

- at least one institution of higher education or nonprofit training organization, and
- at least one local employer or owner or operator of critical infrastructure.

Funding

In FY 2024, an unspecified amount of funding is available to support up to 18 awards for up to $200,000 per award through this program. Project performance periods will span up to two years.

Matching and Cost Sharing

Applicants must provide a 50 percent nonfederal cost share.

Contact Information

Danielle Santos
202-308-3909
nice@nist.gov

https://www.grants.gov/web/grants/view-opportunity.html?oppId=348550

FEDERAL
GRANT PROFILE

Department: U.S. Department of Defense
Agency: Air Force Research Laboratory

FY 2020-2025 Future Scholars for Science, Technology, Engineering, and Mathematics (STEM) Workforce Development Programs

Grant Overview

This program improves the capacity of education systems and communities to create impactful science, technology, engineering, and mathematics (STEM) educational experiences for students and teachers, and to prepare the 21st century STEM workforce. The program intends to address geographic disparities in STEM workforce availability and broaden participation for under-represented and underserved communities. Eligible applicants are institutions of higher education, nonprofit institutions and organizations, states, local governments, and Indian tribes.

Program History

Program history is not available.

Key Information

Total Funding: $50 million
Award Range: $25,000 to $25 million
Match: Not required
Solicitation date: June 17, 2020
Proposal due: July 22, 2024

- Applications will be accepted on a rolling basis through the application deadline

https://www.grants.gov/web/grants/view-opportunity.html?oppId=327212

Tips

- Prior to submitting a proposal, applicants are required to submit a Letter of Intent
- Projects on certain Air Force Materiel Command (AFMC), installations will receive preference
- Funding agency priorities include intelligence/machine learning, biotechnology, and cyber security

Department: U.S. Department of Defense
Agency: Air Force Research Laboratory (AFRL)

FY 2020-2025 Future Scholars for Science, Technology, Engineering, and Mathematics (STEM) Workforce Development Programs

Detailed Summary

The purpose of this program is to improve the capacity of education systems and communities to create impactful science, technology, engineering, and mathematics (STEM) educational experiences for students and teachers, and to prepare the 21st century STEM workforce. The program intends to address geographic disparities in STEM workforce availability and broaden participation for under-represented and underserved communities. The program also aims to:

- Foster community engagement that supports and encourages STEM learning and understanding and builds STEM skills and literacy in an evidence-based and innovative manner
- Increase awareness of the funding agency's science and technology priorities, such as artificial intelligence/machine learning, biotechnology, cyber security, and defense-related science and technologies
- Develop partnerships with industry and other organizations to promote sustainable STEM workforce development programs or projects

The program's objectives are to:

- Provide opportunities for intellectual challenge and collaboration by promoting scientific interactions between the academic community and scientists at the funding agency’s laboratories and facilities
- Develop and maintain a long-term recruiting pipeline supporting the funding agency's laboratories and facilities by training and educating the next generation of scientists and engineers in fundamental research relevant to the funding agency
- Support graduate students pursuing advanced degrees in areas of relevance to STEM literacy, innovation, and employment
- Provide program participants with exposure to researchers and the environment at the funding agency's laboratories and facilities; and to make participants aware of future career and employment opportunities at the funding agency

Projects may include:

- Internships (high school through doctoral)
- Fellowship apprentice/residency programs
- College or university project-based learning programs
- Formal or informal workforce development programs or projects that align with the federal STEM strategy and the funding agency's STEM mission

Applicant Eligibility

Eligible applicants are institutions of higher education, nonprofit institutions and organizations, states, local governments, and Indian tribes.

University-Affiliated Research Centers (UARCs) are eligible to apply, unless precluded from doing so by their Department of Defense UARC contract.

Anticipated places of performance include but are not limited to AFRL's Air Force Materiel Command (AFMC), installations located at:

- Directed Energy Directorate (RD), Kirtland AFB, NM
- Space Vehicles Directorate (RV), Kirtland AFB, NM
- Munitions Directorate (RW), Eglin AFB, FL
- Air Vehicles Directorate (RB), Wright Patterson AFB, OH
- Propulsion Directorate (RZ), Wright Patterson AFB, OH
- 711 Human Performance Wing (RH), Wright Patterson AFB, OH
- Information Directorate (RI), Rome, NY

Funding

In FY 2020-2025, an estimated $50 million is expected to be available to support grants and/or cooperative agreements ranging from $25,000 to $25 million through this program.

Matching funds are not required for this program.

The total award period for this program will begin on October 26, 2020, and end on October 27, 2025. Project periods may not exceed 60 months in length. Applicants must submit a separate budget for each year of their projects. Funding beyond the first year is contingent upon project performance, funding availability, and several other factors. Extensions of project periods may be allowed.

Contact Information

Sara Telano
Contracting Specialist
(505) 853-7353
sara.telano@us.af.mil

Lauren J. Davis
Contracting Specialist
(505) 846-8060
lauren.davis.10@us.af.mil

https://www.grants.gov/web/grants/view-opportunity.html?oppId=327212

FEDERAL
GRANT PROFILE

Department: U.S. Department of Energy
Agency: Office of Cybersecurity, Energy Security, and Emergency Response

FY 2024 Bipartisan Infrastructure Law (BIL) Rural and Municipal Utility Cybersecurity (RMUC) Advanced Cybersecurity Technology (ACT)

Grant Overview

This program will increase the security, reliability, and resiliency of our energy infrastructure. Investments will improve energy resilience in rural communities, decrease energy burdens on utility members and customers, and increase the cybersecurity knowledge, skills, and abilities of utility employees in rural communities. Eligible applicants are rural electric cooperatives; utilities owned by a political subdivision of a State, such as a municipally owned electric utility; utilities owned by any agency, authority, corporation, or instrumentality of one or more political subdivisions of a State.

Program History

This is a new program created through the Infrastructure Investment and Jobs Act.

Key Information

Total Funding: $70 million
Award Range: Varies based on topic area
Match: Varies based on topic area
Solicitation Date: November 16, 2023
Proposal due: January 10, 2024 (Pre-application), April 24, 2024 (Full Application)

Office of Cybersecurity, Energy Security, and Emergency Response | Department of Energy

Tips

- The funding agency will host an informational webinar on December 19, 2023, at 1:00 pm ET.
- Only applicants who are invited to apply based on their pre-applications are eligible to submit a full application.
- Projects that improve the cybersecurity of the utility's (or utilities') operational technology (OT) or industrial control systems (ICS), and/or increase the participation of eligible utilities in cybersecurity threat information sharing programs are strongly encouraged.

Department: U.S. Department of Energy
Agency: Office of Cybersecurity, Energy Security, and Emergency Response

FY 2024 Bipartisan Infrastructure Law (BIL) Rural and Municipal Utility Cybersecurity (RMUC) Advanced Cybersecurity Technology (ACT)

Detailed Summary

The purpose of this program is to increase the security, reliability, and resiliency of our energy infrastructure. Investments will improve energy resilience in rural communities, decrease energy burdens on utility members and customers, and increase the cybersecurity knowledge, skills, and abilities of utility employees in rural communities. These investments will help maximize the benefits of the clean energy transition by facilitating secure grid modernization deployments as the nation works to curb the climate crisis, empower workers, and advance environmental justice.

The goals of the program are to:

- Deploy advanced cybersecurity technologies for electric utility systems
- Increase the participation of eligible entities in cybersecurity threat information sharing programs

Priority will be given to applicants that:

- Have limited cybersecurity resources.
- Owns assets critical to the reliability of the bulk power system; or
- Owns defense critical electric infrastructure.

Funding is available under three distinct topic areas:

Topic Area 1 - Advanced Cybersecurity Technologies (ACT) for Distribution, Generation, and Transmission Utilities: This Topic Area will provide direct support to eligible utilities interested in making significant modifications and investments that enhance “the security posture of electric utilities.” Projects must address the following objectives:

- Improve the cybersecurity posture of the utility’s operational systems;
- Include an appropriate balance of investments in staff, processes, and technologies;
- Improve the effective use of already installed tools and technologies when appropriate;
- Increase participation and engagement of the utility in cybersecurity threat information sharing programs; and
- Implement solutions that have a high likelihood of continued use and effectiveness after the project funding ends

Topic Area Topic Area 2 - Strengthening the Peer-to-Peer and Not-for-Profit Technical Assistance Ecosystem: This Topic Area will support investments that strengthen the community of eligible entities that are currently providing information technology (IT) and cybersecurity support to eligible electric cooperative and municipal utilities and meet the legislative intent to enhance the security posture of electric utilities. Funding can be requested for activities that will improve the cybersecurity posture of utilities by increasing the scope of appropriate, affordable, and accessible products and services provided, including but not limited to purchases of IT and cybersecurity tools and services, technical assistance, and training. Funding can also be requested to enhance the ability of entities to provide products and services and increasing the number of eligible utilities benefiting from the products and services provided. This Topic Area will also provide funding to promote and facilitate the replication of effective service models to other utilities and not-for-profit partners interested in providing products and services to eligible cooperative and municipal utilities.

Topic Area 3 - Increasing Access to Technical Assistance and Training for Utilities with Limited Cybersecurity Resources: This Topic Area will support investments that can strengthen the community of eligible entities that are currently providing IT and cybersecurity support to eligible cooperative and municipal utilities. Applications under Topic Area 3 must focus on improving the knowledge, skills, and abilities of utility participants and cannot include the purchase of cybersecurity tools, technologies, or related assets. This Topic Area will improve the cybersecurity posture of utilities with limited cybersecurity resources by:

- Increasing the scope of appropriate, affordable, and accessible technical assistance and training services provided by eligible entities;
- Enhancing the ability of eligible entities to provide services; and
- Increasing the number of utilities benefiting from the services. This Topic Area is also focused on supporting efforts to promote and facilitate the replication of effective service models in other eligible entities interested in providing services to electric cooperative and municipal utilities.

Projects that include the purchase of tools, technologies, or training must be based on the results of cybersecurity risk assessments. Proposed solutions must address prioritized cybersecurity risks using an approach that includes investments in people and process solutions as well as the technology component of the solution. All projects must describe and demonstrate an ability of the utility to appropriately maintain and manage solutions after the project funding ends.

Applicant Eligibility

Eligible applicants include rural electric cooperatives; utilities owned by a political subdivision of a State, such as a municipally owned electric utility; utilities owned by any agency, authority, corporation, or instrumentality of one or more political subdivisions of a State. Investor-owned electric utilities that sell less than 4,000,000 megawatt hours of electricity per year are also eligible.

Additionally, not-for-profit entities that are in partnership with at least six of the entities described above are eligible to apply under topic area 1 and topic area 2.

Utilities may submit more than one Pre-Application to any of the three Topic Areas provided that each Pre-Application describes a unique, distinct project. Utilities may also submit only one Full Application to each Topic Area provided that each Application describes a unique, distinct project; and may participate as

subrecipients or as Participating Utilities in Topic Areas 2 or 3 on more than one application, provided that each application describes a unique, distinct project.

Funding

The funding agency expects to make a total of approximately $70 million of federal funding available for new cooperative agreements through this program, subject to the availability of appropriated funds. Funding for each topic area is as follows:

- Topic Area 1 - Advanced Cybersecurity Technologies (ACT) for Distribution, Generation, and Transmission Utilities: Approximately $20 million is available to support 10 awards of up to $2 million
- Topic Area 2 - Strengthening the Peer-to-Peer and Notfor-Profit Technical Assistance Ecosystem: Approximately $30 million is available to support 10 awards of up to $3 million
- Topic Area 3 - Increasing Access to Technical Assistance and Training for Utilities with Limited Cybersecurity Resources: Approximately $20 million is available to support 10 awards of up to $2 million

The estimated period of performance for each award will be approximately 24-48 months.

Matching and Cost Sharing

A minimum of 5 percent non-federal cost share is required by applicants for projects related to topic areas 1 and 2; no match is required for projects related to topic area 3. Applicants may propose a cost share of more than 5 percent which could result in higher total award values.

Contact Information

Program Staff
DE-FOA-0002986@netl.doe.gov

Office of Cybersecurity, Energy Security, and Emergency Response | Department of Energy

FEDERAL
GRANT PROFILE

Department: U.S. Department of Homeland Security
Agency: Federal Emergency Management Agency

FY 2023 Homeland Security National Training Program Continuing Training Grants

Grant Overview

The purpose of this program is to support building, sustaining, and delivering core capabilities through the development and delivery of training to achieve the National Preparedness Goal, which is a secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk. Eligible recipients are states, local governments, Federally recognized Indian Tribal governments, nonprofits, institutions of higher education, and nonprofit national associations and organizations.

Program History

Year	Total Funding	# of Awards
2022	$6 million	5
2021	$6 million	5

Key Information

Total Funding: $6 million
Award Range: Up to $6 million
Match: Not required
Solicitation date: June 22, 2023
Proposal due: August 9, 2023

More information can be found here.

Awardee Profile

University of Texas, San Antonio, Texas

AMOUNT: $3,015,000
YEAR: 2016

The University of Texas at San Antonio, representing the National Cybersecurity Preparedness Consortium, received funding to provide research-based, cybersecurity-related training, exercises and technical assistance to local jurisdictions, counties, states and the private sector.

Department: U.S. Department of Homeland Security
Agency: Federal Emergency Management Agency

FY 2023 Homeland Security National Training Program Continuing Training Grants

Detailed Summary

The purpose of this program is to support building, sustaining, and delivering core capabilities through the development and delivery of training to achieve the National Preparedness Goal, which is a secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk. Specifically, this program provides funding for eligible applicants to support and target training solutions for state, local, tribal, and territorial (SLTT) partners, supporting the objective of the National Preparedness System to facilitate an integrated, whole community, risk-informed, capabilities-based approach to preparedness.

The focus areas of this program include:

- Rural preparedness for equitable outcomes: applicants must describe the linkage between gaps identified in their needs analysis and proposed training while considering interdependencies and strategies for integrating all sectors into community emergency preparedness and response efforts; applications must address the following training objectives:
    - Climate Literacy
    - Rural Public Health/Pandemic Preparedness
    - Continuity of Operations Plans and Continuity of Government for Rural Jurisdictions
    - Crisis Management for Rural School Based Incidents
    - Under this focus area, FEMA applies the definition of “rural” as all population, housing, and territory not included within an “urban area” as delineated by the Census Bureau where “urban area” refers to areas of 50,000 or more population and urban clusters of at least 2,500 and less than 50,000 population.
- Build Tribal capacities and capabilities to improve readiness and resilience: application proposals should focus on the preparedness gaps common for Tribal Nations that can be addressed through training. Proposals should address the following topics, relevant to Tribal Nations:
    - Building an Effective Emergency Management Program
    - Climate Literacy
    - Community Engagement
    - Risk Communication Strategies
    - Access to Disaster Risk Reduction Resources

The strategic goal objectives of both focus areas are to:

- Achieve equitable outcomes for those served

- Strengthen the emergency management workforce

Examples of learning solutions under both focus areas include:

- Online training
- In-person instructor-led training
- Synchronous, virtual instructor-led training
- Asynchronous, virtual instructor-led training
- Facilitated workshops and seminars

Applications must include innovative training approaches and concepts that can help solve the tough problems that the nation's emergency management community is expected to confront. These innovations should be replicable, satisfy a specific need, and include processes where new ideas result in useful products.

Applicant Eligibility

Eligible applicants are state and local governments, Federally recognized Indian Tribal governments, nonprofits with 501(c)(3) Internal Revenue Status, nonprofit private institutions of higher education, nonprofit national associations and organizations, and public and state-controlled institutions of higher education.

Applicants must currently administer an existing training program, consistent with the National Incident Management System (NIMS), relevant to the selected focus area(s), or have demonstrable expertise to create and administer a training program capable of developing and delivering training for a national whole community audience, relevant to the selected focus area(s).

Funding

In FY 2023, approximately $6 million of funding is available to support 3-5 awards through this program. Award amounts will vary based on the number of immigrants served through the program.

The project period will span 36 months from September 1, 2023, to August 31, 2026.

Matching Funds and Cost Sharing

There is no cost share or match requirement for this program.

Contact Information

Jessica Sterling
(202) 212-3042
Jessica.sterling@fema.dhs.gov

https://www.grants.gov/web/grants/view-opportunity.html?oppId=348866

FEDERAL
GRANT PROFILE

Department: U.S. Department of Homeland Security
Agency: Federal Emergency Management Agency (FEMA)

FY 2023 Port Security Grant Program (PSGP)

Grant Overview

The Port Security Grant Program supports increased portwide risk management and protect critical surface transportation infrastructure from acts of terrorism, major disasters, and other emergencies. Funding will support port authorities; facility operators; and state, local, and territory agencies for activities associated with implementing area maritime security plans (AMSP), facility security plans (FSPs), vessel security plans (VSPs), and other portwide risk management efforts. Eligible applicants are entities subject to an area maritime security plan, including port authorities, facility operators, and state and local government agencies.

Program History

	Total Funding
2022	$100 million

Key Information and Tips

Total Funding: $100 million
Award Range: Unspecified
Match: 25 percent
Solicitation date: February 27, 2023
Proposal due: May 18, 2023

- Additional consideration will be given to projects certified by the U.S. Coast Guard Captain of the Port (COTP) as having a port-wide benefit.

https://www.fema.gov/grants/preparedness/port-security

Awardee Profile

Municipality of Anchorage, AK

AMOUNT: $1,687,687
YEAR: 2021

Municipality of Anchorage/Port of Alaska received funding through the PSGP to support increased portwide risk management and protect critical surface transportation infrastructure from acts of terrorism, major disasters, and other emergencies.

Department: U.S. Department of Homeland Security
Agency: Federal Emergency Management Agency (FEMA)

FY 2023 Port Security Grant Program (PSGP)

Detailed Summary

The purpose of this program is to support increased port-wide risk management and protect critical surface transportation infrastructure from acts of terrorism, major disasters, and other emergencies. Funding will support port authorities; facility operators; and state, local, and territorial agencies for activities associated with implementing area maritime security plans (AMSP), facility security plans (FSPs), vessel security plans (VSPs), and other port-wide risk management efforts.

For FY 2023, the two areas that will attract the greatest concern by the funding agency are:

- Enhancing cybersecurity, including:
  - Cybersecurity risk assessments
  - Projects that address vulnerabilities identified in cybersecurity risk assessments
- Enhancing the protection of soft targets/crowded places, including:
  - Physical security enhancements at cruise and ferry terminals
  - Enhancements of security aboard ferries
  - Rapid-response boats for preventing or responding to security incidents on waterways

Projects that address these two areas of greatest concern will receive priority during the application evaluation process.

Secondary priority will be given to projects under the following areas:

- Effective planning, including:
  - Development of port-wide security risk management, continuity of operations, and response plans
  - Efforts to strengthen governance integration between/among regional partners
  - Assessment of capabilities and gaps in planning for the needs of persons with disabilities and others with access and functional needs
- Training and awareness campaigns, including:
  - Active shooter training
  - Shipboard firefighting training
  - Public awareness/preparedness campaigns
  - Maritime domain awareness projects
- Equipment and capital projects, including:
  - Implementing risk management projects that support port resilience and recovery
  - Implementing physical security enhancement projects
  - Transportation Worker Identification Credential (TWIC) projects
- Exercises, including response exercises

Applicant Eligibility

Eligible applicants are entities subject to an area maritime security plan (AMSP), as defined by Title 46, Section 70103(b) of the U.S. Code (U.S.C.), including port authorities. Eligible applicants include but are not limited to port authorities, facility operators, and state, local, and territorial government agencies.

For the purposes of this program, a facility operator is defined as an entity that 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, including terminal operators, ferry systems, bar/harbor pilots, and merchant's exchanges.

Eligibility for funding of explosives detection canine teams (EDCTs) is restricted to:

- U.S. ferry systems regulated under Title 33 of the Code of Federal Regulations (C.F.R.) Parts 101, 103, and 104, and the passenger terminals these specific ferries service under 33 C.F.R. Part 105
- Maritime Transportation Security Act (MTSA)-regulated facilities
- Port authorities, port police, and local law enforcement agencies that provide direct layered security for these U.S. ferry systems and MTSA-regulated facilities and are defined in the AMSP, facility security plans (FSPs), or vessel security plans (VSPs)

All applicants must be fully compliant with relevant maritime security regulations under Title 33, Parts 101-106 of the C.F.R.

Prior to receiving awards, award recipients must ensure and maintain adoption and implementation of the National Incident Management System (NIMS).

An eligible entity may submit no more than one application within each port area. Large projects that implement multiple components in multiple port areas should be submitted as separate applications. The funding agency will generally view multiple agencies within a local government operating within one port area as a single eligible entity. An eligible entity operating multiple facilities, departments, subcomponents, or agencies within a single port area may choose to submit separate applications for facilities, departments, subcomponents, or agencies within it; however, any such separate applications will be considered part of the same eligible entity for purposes of the program's matching requirements. In general, each individual facility, department, subcomponent, or agency of a single eligible entity should submit no more than one application.

Funding

In FY 2023, a total of $100 million is available to support an unspecified number of awards through this program.

In general, all applicants, with the exception of private, for-profit entities, must provide at least 25 percent of the total project costs via nonfederal cash and/or in-kind contributions. Applicants that are private, for-profit entities must provide at least 50 percent of the total project costs via nonfederal cash and/or in-kind contributions.

The following exceptions to the match requirements may apply:

- Projects that have a port-wide benefit need only be funded at the public sector matching level, regardless of applicant entity type
- Matching funds are not required for applicants whose total project requests are less than $25,000

- Matching funds are not required for projects that train public safety personnel in the enforcement of security zones or in assisting in the enforcement of such security zones

The project period will span 36 months, with a project start date of September 1, 2023, and a projected end date of August 31, 2026. The funding agency may consider formal, written requests with compelling justifications. Extension requests must be submitted at least 120 days prior to the end of the project period.

Costs for the acquisition, operation, and maintenance of security equipment or facilities to be used for security monitoring and recording, security gates and fencing, marine barriers for designated security zones, security-related lighting systems, remote surveillance, concealed video systems, security vessels, and other security-related infrastructure or equipment that contributes to the overall security of passengers, cargo, or crew members is limited to $1 million per project; however, this limitation does not apply to projects funded under other provisions of Section 70107 of the U.S.C.

Costs for explosive detection canine teams (EDCTs) are limited to $150,000 per year for three years, for a total of $450,000. Management and administration (M&A) costs are limited to 5 percent of the total award amount.

Applicants must obtain approval from the funding agency for construction or renovation projects.

Contact Information

Program Staff
(800) 368-6498
askcsid@fema.dhs.gov

https://www.fema.gov/grants/preparedness/port-security

FEDERAL
GRANT PROFILE

Department: U.S. Department of Homeland Security
Agency: Federal Emergency Management Agency (FEMA)

FY 2023 State Homeland Security Program (SHSP)

Grant Overview

The purpose of this program is to enhance the ability of state, local, tribal, and territorial governments as well as nonprofit organizations to prevent, protect against, and respond to terrorist attacks. Eligible applicants are all 56 U.S. states and territories which includes any state, 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.

Program History

	Total Funding	# of Awards
2020	$415 million	56
2019	$415 million	56

Key Information and Tips

Total Funding: $415 million
Match: Not required
Solicitation date: February 27, 2023
Proposal due: May 18, 2023

Applicants are required to complete a threat and hazard identification and risk assessment (THIRA)/stakeholder preparedness review (SPR)

https://www.fema.gov/grants/preparedness/homeland-security

Awardee Profile

Commonwealth of Virginia

AMOUNT: $9.2 million
YEAR: 2019

The Commonwealth of Virginia received formula funding through this program to prevent, prepare for, protect against, and respond to acts of terrorism.

Department: U.S. Department of Homeland Security
Agency: Federal Emergency Management Agency (FEMA)

FY 2021 State Homeland Security Program (SHSP)

Detailed Summary

The purpose of this program is to enhance the ability of state, local, tribal, and territorial governments as well as nonprofit organizations to prevent, protect against, and respond to terrorist attacks. This program is part of the funding agency's larger comprehensive set of measures to strengthen the nation's communities against potential terrorist attacks.

All assets supported in part or entirely through this program must be readily deployable and National Incident Management System (NIMS)-typed, when possible, to support emergency or disaster operations per existing Emergency Management Assistance Compact (EMAC) agreements.

All emergency communications investments must align with needs identified in the applicant's statewide communication interoperability plan (SCIP). Applicants must also coordinate with their statewide interoperability coordinator (SWIC) and/or statewide interoperability governing body (SIGB) when developing the emergency communications investment.

Funding will be provided for the following program components:

- (Part A): State Homeland Security Program (SHSP)
- (Part D): Urban Area Security Initiative (UASI)
- (Part G): Operation Stonegarden (OPSG)

The purpose of the State Homeland Security Program (SHSP) component is to support state, local, tribal, and territorial (SLTT) efforts to build, sustain, and deliver the capabilities necessary to prevent, prepare for, protect against, and respond to acts of terrorism.

For FY 2023, this program is focused on the criticality of information sharing and collaboration to building a national culture of preparedness and protecting against terrorism and other threats to national security. All projects must address the following identified priority areas related to the most serious threats to the nation:

- Enhancing the protection of soft targets/crowded places
- Enhancing information and intelligence sharing and analysis
- Combating domestic violent extremism
- Enhancing cybersecurity
- Enhancing community preparedness and resilience
- Enhancing election security

Funding will also support activities to address capability gaps identified through the threat and hazard identification and risk assessment (THIRA) and stakeholder preparedness review (SPR) process. Applicants should also consider allocating funding across core capability gaps and national priorities to address the following enduring security needs that will help the implementation of a comprehensive approach to securing communities:

- Effective planning
- Training and awareness campaigns
- Equipment and capital projects
- Exercises

All applicants must complete a THIRA/SPR and prioritize funds to support building capability, closing capability gaps, or sustaining capabilities that address national priorities and/or support enduring security needs. Additional information on the THIRA/SPR process, including other National Preparedness System (NPS) tools and resources, can be found online at www.fema.gov/emergency-managers.

All projects must have a demonstrated nexus to achieving target capabilities related to preventing, preparing for, protecting against, and responding to acts of terrorism; however, projects may also simultaneously support enhanced preparedness for disasters unrelated to acts of terrorism.

All applicants must develop formal investment justifications (IJs) that address the proposed investments. Applicants must propose at least 5 and up to 12 investments. Within each investment, applicants must propose at least one project. There is no limit to the number of projects that may be submitted.

Applicants must propose at least one respective project for each of the five aforementioned priority areas with a minimum spend requirement, except for the enhancing cybersecurity priority area. All projects associated with the minimum spend of a priority area must be submitted in the same IJ.

Applicants must also identify a fusion center project that will indicate alignment to a designated fusion center. Applicants must coordinate with the designated fusion center when developing the fusion center project.

Applicant Eligibility

Eligible applicants are all 56 U.S. states and territories which includes any state, 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.

The state administrative agency (SAA) is the only entity eligible to submit applications.

In general, applicants must belong to, be in, or act as a temporary member of Emergency Management Assistance Compact (EMAC), except for American Samoa and the Commonwealth of the Northern Mariana Islands.

All applicants must develop formal investment justifications (IJs) that address the proposed investments. Applicants must propose at least 5 and up to 12 investments. Within each investment, applicants must propose at least one project. There is no limit to the number of projects that may be submitted.

Applicants must propose at least one respective project for each of the five identified priority areas with a minimum spend requirement, as detailed in the Summary section, except for the enhancing cybersecurity priority area. All projects associated with the minimum spend of a priority area must be submitted in the same IJ.

Applicants must also identify a fusion center project that will indicate alignment to a designated fusion center.

Funding

In FY 2023, $1.12 billion is available to support approximately 56 awards for this program overall, with $415 million available to support awards through this component.

Funding selections are anticipated to be made by July 21, 2023, and awards are anticipated to be made by September 30, 2023.

The project period will last 36 months, from September 1, 2023, to August 31, 2026. Requests for extensions to the project period will be considered.

The recipient state administrative agency (SAA) must pass through at least 80 percent of the total award amount to local or tribal units of government within 45 calendar days of receipt of funds.

Matching and Cost Sharing

Matching funds are not required for this program.

Award recipients must allocate at least 30 percent of the total award amount to address identified priority areas. Award recipients must allocate funds to each priority area according to the following minimum spend requirements:

- Enhancing the protection of soft targets/crowded places: at least 3 percent of the total award amount
- Enhancing information and intelligence sharing and analysis: at least 3 percent of the total award amount
- Combating domestic violent extremism: at least 3 percent of the total award amount
- Enhancing cybersecurity: no minimum allocation amount
- Enhancing community preparedness and resilience: at least 3 percent of the total award amount
- Enhancing election security: at least 3 percent of the total award amount

Award recipients will have the flexibility to allocate the remaining 15 percent of the required allocation across the priority areas.

Award recipients must allocate the remaining 70 percent of the total award amount to address capability gaps identified through their threat and hazard identification and risk assessment (THIRA) and stakeholder preparedness review (SPR) process.

In addition, at least 35 percent of total funding awarded under this component and the Urban Area Security Initiative (UASI) component of this program must be allocated to law enforcement terrorism prevention activities (LETPAs).

Management and administration (M&A) costs are limited to 5 percent of the total award amount.

Costs for personnel activities, including operational overtime costs, are limited to 50 percent of the total award amount.

Contact Information

Program Staff
(800) 368-6498
AskCSID@fema.dhs.gov

https://www.fema.gov/grants/preparedness/homeland-security

FEDERAL
GRANT PROFILE

Department: U.S. Department of Homeland Security
Agency: Federal Emergency Management Agency (FEMA)

FY 2023 State and Local Cybersecurity Grant Program

Grant Overview

The purpose of this program is to strengthen the cybersecurity practices and resilience of state, local, and territorial (SLT) governments. Eligible applicants are all 56 states and territories, including any state of the United States, the District of Columbia, American Samoa, Guam, the Commonwealth of the Northern Mariana Islands, the Commonwealth of Puerto Rico, and the U.S. Virgin Islands.

Program History

	Total Funding	# of Awards
2021	$160 million	61

Key Information

Total Funding: $374.9 million
Award Range: Varies
Match: 20 percent
Solicitation date: August 7, 2023
Proposal due: October 6, 2023

https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program

Tips

- Only one application may be submitted by each eligible entity, and no more than four investment justifications may be submitted with the application.
- Multiple eligible entities may group together to address cybersecurity risks and threats to information systems within the states and territories that are the eligible entities.

Department: U.S. Department of Homeland Security
Agency: Federal Emergency Management Agency

FY 2023 State and Local Cybersecurity Grant Program

Detailed Summary

The purpose of this program is to strengthen the cybersecurity practices and resilience of state, local, and territorial (SLT) governments. This program enables the funding agency to make targeted cybersecurity investments in SLT governments, thus improving the security of critical infrastructure and improving the resilience of the services SLT governments provide their communities.

Applicants are required to focus on addressing the following program objectives in their applications:

- Objective 2: understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments
- Objective 3 implement security protections commensurate with risk
- Objective 4: ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility

Award recipients will be required to develop a cybersecurity plan, establish a cybersecurity planning committee to support development of the plan, and identify projects to implement using program funding. Cybersecurity plans must include the following activities:

- Conducting assessments and evaluations as the basis for individual projects throughout the life of the program
- Adopting key cybersecurity best practices and consulting the cybersecurity performance goals (CPGs) detailed online at www.cisa.gov/cross-sector-cybersecurity-performance-goals

Funding may be used for developing, updating, and implementing a cybersecurity plan. Allowable investments made in support of this goal must fall into the categories of planning, organization, equipment, training, or exercises (POETE), aligned to closing capability gaps or sustaining capabilities.

Applicant Eligibility

Eligible applicants are all 56 states and territories, including any state of the United States, the District of Columbia, American Samoa, Guam, the Commonwealth of the Northern Mariana Islands, the Commonwealth of Puerto Rico, and the U.S. Virgin Islands. Applications must be submitted by the governor-designated state administrative agency (SAA).

Multiple eligible entities may group together to address cybersecurity risks and threats to information systems within the states and territories that are the eligible entities. The multientity project submissions must be approved by each of the participating state or territory's cybersecurity planning committees, and each of the multientity project submissions must be aligned with each of the participating state's or territory's respective cybersecurity plan.

Only one application may be submitted by each eligible entity, and no more than four investment justifications may be submitted with the application.

Funding

In FY 2023, a total of $374,981,324 is available to support 56 awards through this program. Each state and territory will receive a baseline allocation using thresholds established in section 2200A(1) of the Homeland Security Act of 2022. Project periods will be for up to 36 months from the date of the award.

The project period is 48 months and is expected to begin on December 1, 2023, and end on November 30, 2027. Extension requests will be granted only due to compelling legal, policy, or operational challenges.

Matching and Cost Sharing

In general, applicants must provide at least 20 percent of the total project costs via cash or in-kind contributions. The matching requirement for multientity projects is 10 percent. The matching requirement applies to each individual project funded by the award, rather than just the cumulative total.

The matching requirement is waived for the insular areas of the U.S. territories of American Samoa, Guam, the Commonwealth of the Northern Mariana Islands, and the U.S. Virgin Islands. In addition, the matching requirement may be waived or modified for entities demonstrating economic hardship.

In general, award recipients must pass through at least 80 percent of the total award amount. With the consent of the recipients, this pass-through may be in the form of in-kind services, capabilities, or activities, or a combination of funding and other services. In addition, 25 percent of the total award amount must go to rural areas.

Management and administrative (M&A) costs are limited to 5 percent of the total award amount.

Pre-award costs are allowable only with the prior written approval of the funding agency and as included in the award agreement.

Contact Information

Questions should be directed to the appropriate program contact listed on pages 49-50 of the NOFA file.

https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program

FEDERAL

GRANT PROFILE

Department: Homeland Security, Department of (DHS)

Agency: Federal Emergency Management Agency

FY 2023 Transit Security Grant Program

Grant Overview

This program is intended to protect critical surface transportation infrastructure and the traveling public from acts of terrorism and to increase transportation infrastructure resilience. In assessing the national risk profile for FY 2023, the funding agency has identified enhancing cybersecurity and enhancing the protection of soft targets/crowded places as areas of highest concern. Eligible applicants are governmental agencies with eligible rail, intra-city bus, and ferry systems. Eligible transit agencies are determined based on daily unlinked passenger trips and transit systems that serve historically eligible Urban Area Security Initiative (UASI) jurisdictions.

Program History

	Total Funding	# of Awards
2020	$13 million	24

Key Information

Total Funding: $93 million
Award Range: Unspecified
Match: Not required
Solicitation Date: February 27, 2023
Proposal Due Date: May 18, 2023

- Award recipients will be required to participate in a regional transit security working group (RTSWG) or develop an RTSWG if one does not already exist. The RTWSG should serve as a forum of regional partners to discuss risk, planning efforts, and mitigation strategies

https://www.fema.gov/grants/preparedness/transit-security

Awardee Profile

Chicago Transit Authority, Chicago, IL

AMOUNT: $14.8 million
YEAR: 2020
The Chicago Transit Authority received funding to increase the security and resiliency of transit in the Chicago metro area.

Department: Homeland Security, Department of (DHS)

Agency: Federal Emergency Management Agency

FY 2023 Transit Security Grant Program

Detailed Summary

The purpose of this program is to protect critical surface transportation infrastructure and the traveling public from acts of terrorism and to increase transportation infrastructure resilience.

In assessing the national risk profile for FY 2023, the funding agency has identified these two areas of highest concern:

- Enhancing cybersecurity: eligible project types include:
  - Cybersecurity risk assessments
  - Projects that address vulnerabilities identified in cybersecurity risk assessments

- Enhancing the protection of soft targets/crowded places: eligible project types include:
  - Physical security enhancements at rail or bus stations located in historically eligible Urban Area Security Initiative (UASI) urban areas
  - Use of visible, unpredictable deterrence, including operational packages
  - Directed/surge patrols on overtime
  - Explosive detection canine teams

Likewise, there are several enduring security needs that crosscut the homeland security enterprise. The following are second-tier priorities that help recipients implement a comprehensive approach to securing critical transportation infrastructure:

- Effective planning: examples of eligible project types include:
  - Development of system-wide security risk management plans, continuity of operations plans, and response plans/station action plans; as well as system-wide and/or asset-specific vulnerability assessments
  - Efforts to strengthen governance integration between/among regional partners
  - Assessment of capabilities and gaps in planning for the needs of persons with disabilities and others with access and functional needs

- Training and awareness campaigns: examples of eligible project types include:
  - Active shooter training, including integrating the needs of persons with disabilities
  - Security training for employees, including basic security awareness
  - Public awareness/preparedness campaigns

- Equipment and capital projects: examples of eligible project types include:
  - Top transit asset list risk remediation

- Protection of other high-risk, high-consequence areas or systems that have been identified through system-wide risk assessments
- Chemical, biological, radiological, nuclear, and explosive detection, prevention, response, and recovery equipment
- Security screening equipment and technology for people and baggage
- Unmanned aircraft systems detection technologies
- Exercises: an example of an eligible project type is response exercises

Examples of allowable project costs include:

- Construction and renovation
- Backfill, overtime, and hiring
- Equipment
- Travel
- Maintenance and sustainment
- Authorized use of contractual grant writers and/or grant managers

Applicant Eligibility

Eligible applicants are governmental agencies with eligible rail, intra-city bus, and ferry systems. Eligible transit agencies are determined based on daily unlinked passenger trips and transit systems that serve historically eligible Urban Area Security Initiative (UASI) urban areas.

Certain ferry systems are eligible to apply for funding through this program; however, ferry systems that elect to participate will not be considered for funding through the Port Security Grant Program (PSGP).

Prior to receiving any award funds, recipients must ensure and maintain adoption and implementation of the National Incident Management System (NIMS).

Funding

In FY 2023, a total of $93 million is available to support awards through this program. Matching funds are not required for this program. Management and administrative (M&A) costs are limited to 5 percent of the total award amount. Project periods may span up to 48 months, beginning on September 1, 2023, and ending on August 31, 2026. Extensions to the initial project period may be permitted. Not required

Contact Information

Program Staff
(800) 368-6498
askcsid@fema.dhs.gov

https://www.fema.gov/grants/preparedness/transit-security

FEDERAL
GRANT PROFILE

Agency: National Science Foundation (NSF)
Office: Division of Electrical, Communication, and Cyber Systems

FY 2023 Energy, Power, Control, and Networks (EPCN)

Grant Overview

The purpose of this program is to encourage research on emerging technologies and applications including energy, transportation, robotics, and biomedical devices and systems. Funding will support innovative research in modeling, optimization, learning, adaptation, and control of networked multiagent systems; higher-level decision-making and dynamic resource allocation; and risk management in the presence of uncertainty, subsystem failures, and stochastic disturbances. Eligible applicants include institutions of higher education (IHEs), nonprofit, non-academic organizations, tribal governments, for-profit organizations, and state and local governments may be eligible to apply.

Program History

Since 2015, the program has granted 343 awards.

Key Information and Tips

Total Funding: Unspecified
Match: Not required
Proposal due: Rolling

- Areas of interest for this program include control systems, energy and power systems, power electronics systems, and learning and adaptive systems.

https://new.nsf.gov/funding/opportunities/energy-power-control-networks-epcn-0

Awardee Profile

Columbia University of New York City, NY

AMOUNT: $396,186
YEAR: 2023

Through the NSF grant, Columbia University of New York used machine learning to analyze a large number of storage resources in electricity markets. This research helped create computational tools that will aid in providing affordable and reliable electricity supply in sustainable power systems.

Agency: National Science Foundation (NSF)
Office: Division of Electrical, Communication, and Cyber Systems

FY 2023 Energy, Power, Control, and Networks (EPCN)

Detailed Summary

The purpose of this program is to encourage research on emerging technologies and applications including energy, transportation, robotics, and biomedical devices and systems. Funding will support innovative research in modeling, optimization, learning, adaptation, and control of networked multiagent systems; higher-level decision-making and dynamic resource allocation; and risk management in the presence of uncertainty, subsystem failures, and stochastic disturbances. This program also invests in novel machine-learning algorithms and analysis, adaptive dynamic programming, brain-like networked architectures performing real-time learning, and neuromorphic engineering.

Areas of interest include:

- Control systems:
  - Distributed control and optimization
  - Networked multiagent systems
  - Stochastic, hybrid, non-linear systems
  - Dynamic data-enabled learning, decision, and control
  - Cyber-physical control systems
  - Applications (biomedical, transportation, or robotics)

- Energy and power systems:
  - Solar, wind, and storage devices integration with the grid
  - Monitoring, protection, and resilient operation of grid
  - Power grid cybersecurity
  - Market design, consumer behavior, and regulatory policy
  - Microgrids
  - Energy-efficient buildings and communities

- Power electronics systems:
  - Advanced power electronics and electric machines
  - Electric and hybrid electric vehicles
  - Energy harvesting, storage devices, and systems
  - Innovative grid-tied power electronic converters

- Learning and adaptive systems:
  - Neural networks
  - Neuromorphic engineering systems
  - Data analytics and intelligent systems
  - Machine learning algorithms, analysis, and applications

Applicant Eligibility

Eligible applicants include institutions of higher education (IHEs), nonprofit, non-academic organizations, tribal governments, and state and local governments. In addition, for-profit organizations may be eligible to apply if the project is of special concern from a national point of view, special resources are available for the work, or the proposed project is especially meritorious.

Collaborative proposals involving principal investigators from two or more institutions are accepted. Grant Opportunities for Academic Liaison with Industry (GOALI) proposals must include at least one industrial co-principal investigator. Organizations that have previously had a proposal declined must wait at least one year from the date of their initial submission before reapplying.

Funding

In FY 2023, an unspecified amount of funding is available to support an unknown amount of awards through this program.

Matching and Cost Sharing

Matching funds are not required for this program. Inclusion of voluntary committed cost sharing in the budget or budget justification is prohibited; however, applicants may contribute a voluntary uncommitted cost share.

Contact Information

Eyad Abed
(703) 292-8339
eabed@nsf.gov

Mahesh Krishnamurthy
(703) 292-8339
mkrishna@nsf.gov

Aranya Chakrabortty
(703) 292-8113
achakrab@nsf.gov

Anthony Kuh
(703) 292-8339
akuh@nsf.gov

https://new.nsf.gov/funding/opportunities/energy-power-control-networks-epcn-0

Free Resources

Below is a list of free resources that local governments may explore accessing to bolster its cybersecurity practices.

CIS - Multi State Information Sharing and Analysis Center

State, local, tribal and territorial governments in the U.S. are eligible to become a member of the Multi State Information Sharing and Analysis Center. The goals of the center are to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery. The center provides free membership and offers access to a collection of integrated cybersecurity resources such as a 24/7 security operation center, incident response services, and cybersecurity advisories and notifications.

DHS - Nationwide Cybersecurity Review (NCSR)

Cybersecurity assessments are provided through the NCSR program. The NCRS is a no-cost, anonymous, annual self-assessment designed to measure gaps and capabilities of state, local, tribal, and territorial governments' cybersecurity programs. The NCSR evaluates cybersecurity maturity across the nation while providing actionable feedback and metrics directly to individual respondents in state, local, tribal, and territorial governments. The review identifies gaps and develops a benchmark to gauge year-to-year progress, as well as anonymously measuring results across all reviews.

CSIA - Assessment Evaluation and Standardization

The Assessment Evaluation and Standardization program is available to federal, state, local, tribal, and territorial governments, critical infrastructure, and federal agency partners, to train individuals that can perform several cybersecurity assessments and reviews in accordance with industry and/or federal information security standards. The program goals are to produce a workforce of prepared and qualified assessors, ensure that assessors have the knowledge and skills necessary to conduct assessments according to the CISA standards and methodologies, and ensure that assessment results are of high quality, consistent, and repeatable.

CISA - Cyber Infrastructure Survey

The Cyber Infrastructure Survey evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and the overall resilience of an organization's cybersecurity ecosystem. Completing the Cyber Infrastructure Survey will provide an organization with an effective assessment of critical services, cybersecurity controls, an interactive dashboard to support cybersecurity planning and resource allocation, and peer performance data. Interested entities should contact the program contacts at ISDAssessments@cisa.dhs.gov to get started.

CISA - Cyber Resilience Review (CRR)

The CRR program is an interview-based assessment that evaluates an organization's operational resilience and cybersecurity practices. The CRR evaluates the maturity of an eligible entity's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities across the following 10 domains: asset management, controls management, configuration, and change management, vulnerability management, incident management, service continuity management, risk, management, external dependency management, training and awareness, and situational awareness. Receiving a CCR will provide an organization with a more robust awareness of its cybersecurity posture by providing and facilitating improved enterprise-wide awareness of the need for effective cybersecurity management and a review of capabilities essential to the continuity of critical services during operational challenges. This program is offered as either a self-assessment or a CISA facilitated assessment. Interested entities should contact the program contacts at cyberadvisor@cisa.dhs.gov to get started.

CISA - External Dependencies Management (EDM) Assessment

The EDM Assessment program is an interview-based assessment that evaluates an organization's management of external dependencies. This assessment focuses on the relationship between an organization's high-value services

and assets—such as people technology, facilities, and information—and evaluates how the organization manages risks derived from its use of the Information and Communications Technology Supply Chain in the deliverance of services. The EDM Assessment evaluates the maturity and capacity of an organization's external dependencies risk management across relationship formations, relationship management and governance, and service protection and sustainment. Participating in an EDM Assessment will provide an organization with an informed understanding of its ability to respond to external dependency risks by providing and facilitating the opportunity for internal discussion of vendor-related issues and the organization's reliance upon external entities in order to provide services, improvement options for consideration derived from recognized standards and best practices, and a comprehensive report on the organization's third-party risk management practices and capabilities.

CISA - Phishing Campaign Assessment (PCA)

The PCA program measures a workforce's tendency to click on email phishing lures. Eligible entities can use PCA results to inform the anti-phishing training and awareness that they provide to their workforce. The goals of the program are to test and assess the behavioral responses of a specified target user base when presented with expertly crafted phishing emails emulating real world threats and inform the leadership of potential training and awareness improvements based on the metrics gathered through the course of the assessment. Interested entities should contact the program contacts at vulnerability@cisa.dhs.gov to get started.

CISA - Risk and Vulnerability Assessment (RVA)

The RVA program collects data through onsite assessments and combines it with national threat and vulnerability information in order to provide an eligible entity with actionable remediation recommendations prioritized by risk. This assessment's objectives are to identify weaknesses through network, system, and application penetration testing; test stakeholders, using a standard, repeatable methodology to deliver actionable findings and recommendations; and analyze collected data to identify security trends across all RVA stakeholder environments. After completing the Risk and Vulnerability Assessment, the organization will receive a final report that includes business executive recommendations, specific findings, and potential mitigations, as well as technical attack path details. An optional debrief presentation summarizing preliminary findings and observations is also available. Interested entities should contact the program contacts at vulnerability@cisa.dhs.gov to get started.

CISA - Vulnerability Scanning

The Vulnerability Scanning Program continuously assesses the health of internet accessible assets by checking for known vulnerabilities, weak configurations, and suboptimal security practices. The objectives of the program are to maintain enterprise awareness of internet-accessible systems, provide insight into how systems and infrastructure appear to potential attackers, and drive proactive mitigation of vulnerabilities and reduce risk. Interested entities should contact the program contacts at vulnerability@cisa.dhs.gov to get started.