Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

STRENGTHENING CYBERSECURITY

Resources & Technical Assistance

October 16, 2023

Overview

The Infrastructure Recovery Support Function (RSF) within the Interagency Recovery Coordination (IRC) Section of the California Governor's Office of Emergency Services (Cal OES) has created this document to provide an overview of funding opportunities and technical assistance available to support strengthening cybersecurity infrastructure in California.

For more information about the opportunities presented within this document, as well as any questions or concerns, please reach out to us at: LongTermRecovery@caloes.ca.gov.

Current Funding Opportunities

Homeland Security Grant Program

- **Grantor**: California Governor's Office of Emergency Services (Cal OES)
- **Description**: Cal OES acts as the State Administrative Agency (SAA) and administers the federal homeland security funding to the locals for HSGP and Urban Areas Security Initiative (UASI). Cal OES applies for federal funding and upon receipt of the award, Cal OES passes the funding to local jurisdictions. Local agencies may apply for both fund sources if qualifications are met.

  Fifty-eight (58) Operational Areas (OA – counties) and six (6) federally designated Urban Areas (UA) receive HSGP funding through Cal OES and administer the grants at the local level. The local jurisdictions are responsible for determining the priorities of their area.

  For the OAs, a "Body of Five" (County Public Health Officer, County Fire Chief, Municipal Fire Chief, County Sheriff, and City Police) determines how the funds are allocated in their respective jurisdiction. For the UAs (San Diego, Bay Area, Los Angeles/Long Beach, Anaheim/Santa Ana, Riverside, and Sacramento), an Urban Area Working Group (UAWG) makes those same decisions for their regions.
- **Eligibility**: Dependent on eligible Homeland Security Grant Program. Eligible project activities with homeland security funding include Planning, Organization,

Equipment, Training and Exercise and must be linked to the prevention, protection, mitigation, response, or recovery of terrorist events.

- **Application Deadline**: Recurring annual grant. Reach out to Cal OES Homeland Security Grants Unit for more information.
- **Contact Information**:
  - Alissa Adams
  - Phone: (916) 761-5544
  - Email: Alissa.Adams@CalOES.ca.gov
- **Website**: https://www.caloes.ca.gov/office-of-the-director/policy-administration/finance-administration/grants-management/homeland-security-emergency-management-programs/homeland-security-grants-program/

State and Local Cybersecurity Grant Program

- **Agency**: FEMA
- **Description**: The State and Local Cybersecurity Grant Program provides funding to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments.
- **Application Deadline:** Not accepting applications currently
- **Contact**: askcsid@fema.dhs.gov
  - (800) 368-6498
- **Website**: https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program

Technical Assistance & Informational Resources

Critical Infrastructure Vulnerability Assessments

- **Agency**: Cybersecurity and Infrastructure Security Agency (CISA)
- **Description**: The Cybersecurity and Infrastructure Security Agency (CISA) conducts specialized security and resilience assessments on the Nation's critical infrastructure. These voluntary assessments assist CISA and its partners—federal, state, tribal, territorial governments, and private industry—in better understanding and managing risk to critical infrastructure. The assessments examine infrastructure vulnerabilities, interdependencies, capability gaps, and the consequences of their disruption. Vulnerability assessments, combined with infrastructure planning resources developed through the Resilience Planning Program | CISA program, forms an integrated planning and assessment capability. This suite of capabilities, methods, and tools support the efficient and effective use of resources to enhance critical infrastructure resilience to all hazards. There are four types of assessments offered:

    - Security Assessment at First Entry - designed to rapidly evaluate a facility's current security posture and identify options for facility owners and operators to mitigate relevant threats.
    - Infrastructure Survey Tool - is a voluntary, web-based assessment that Protective Security Advisors (PSAs) conduct in coordination with facilities owners and operators to identify and document the overall security and resilience of the facility.
    - Infrastructure Visualization Platform - is a data collection and presentation medium that combines immersive imagery, geospatial information, and hypermedia data of critical facilities and surrounding areas to enhance planning, protection, and response efforts.
    - Regional Resiliency Assessment Program - is a voluntary, cooperative assessment of specific critical infrastructure that identifies a range of security and resilience issues that could have regionally or nationally significant consequences.
- **Contact:** ISDAssessments@cisa.dhs.gov
- **Website**: https://www.cisa.gov/critical-infrastructure-vulnerability-assessments

The Infrastructure Dependency Primer

- **Agency**: Cybersecurity and Infrastructure Security Agency (CISA)
- **Description**: This tool is a supplement to the Infrastructure Resilience Planning Framework and is intended to help state and local planners better understand how infrastructure dependencies can impact risk and resilience in their community and incorporate that knowledge into planning activities. It provides a foundation for understanding critical infrastructure, identifying dependencies, and improving system resilience through planning. It is organized into three primary sections: Learn, Plan, and Implement.
- **Website**: https://www.cisa.gov/idp

Resilience Planning Program

- **Agency**: Cybersecurity and Infrastructure Security Agency (CISA)
- **Description**: The Resilience Planning Program (RPP) works with government officials and infrastructure owners and operators to plan, design, and implement solutions that enhance the security and resilience of critical infrastructure against a variety of threats. The RPP offers an interdisciplinary and partnership-based approach that incorporates resilience strategies and policies into all phases of critical infrastructure planning, design, construction, and maintenance. This holistic approach helps public and private owners and operators, and state, local, tribal, and territorial planners and policy makers effectively prioritize and integrate resilience measures into policies, plans, designs, and operational procedures.
- **Contact:** Resilience_Planning@cisa.dhs.gov
- **Website**: Resilience Planning Program | CISA

Cybersecurity

Critical Infrastructure Exercises

- **Agency**: Cybersecurity and Infrastructure Security Agency (CISA)
- **Description**: The Cybersecurity and Infrastructure Security Agency (CISA) conducts cyber and physical security exercises with government and industry partners to enhance security and resilience of critical infrastructure. These exercises provide stakeholders with effective and practical mechanisms to identify best practices, lessons learned, and areas for improvement in plans and procedures. These exercises may also inform future planning, technical assistance, training, and education efforts. CISA works with partners to design and conduct exercises that range from small-scale, discussion-based exercises to large-scale, operations-based exercises. CISA also offers a wide portfolio of downloadable CISA Tabletop Exercise Packages (CTEPs) to serve as an off-the-shelf solution for a variety of stakeholders' exercise needs.
- **Website**: https://www.cisa.gov/critical-infrastructure-exercises

Independent Security Assessments

- **Agency**: California Department of Technology (CDT)
- **Description**: The ISA is a technical analysis of identified controls designed to measure Cyber Security maturity and are performed by the Cyber Network Defense (CND) Team of the California Military Department. Areas within the current ISA include host vulnerability assessments, firewall analysis, host hardening analysis, phishing susceptibility, network penetration testing, and snap-shot analysis of network traffic for signs of threat actor compromise. The Independent Security Assessment Criteria can be obtained through your entity's designated Information Security Officer.
- **Website**: Resilience Planning Program | CISA

Motorola Solutions – Cybersecurity Grant Assistance Program

- **Organization**: Motorola Solutions
- **Description**: Fill out the form online for customized grant assistance for projects in the Technology & IT, Local Government and Cybersecurity categories. This includes grant research, grant alert notices and grant application reviews from a team of grant experts. Whether you're just starting your project or need to add the final touches to an application, their grant consultants have teamed up with Motorola Solutions - Cybersecurity to provide grant resources and services specific to Technology & IT, Local Government and Cybersecurity. They do not guarantee funding but will do everything they can to assist you in submitting a successful grant application.
- **Application Deadline**: Ongoing
- **Website**: https://www.govgrantshelp.com/motorola-cybersecurity-grant-assistance/?elqTrackId=fbf22c0ee80e4c658b2071fd62194a65&elqaid=5675&elqat=2

Motorola Solutions – Education Government Grant Assistance

- **Organization**: Motorola Solutions
- **Description**: Fill out the form online for customized grant assistance for projects in the Communications category for education. This includes grant research, grant alert notices, and grant application reviews from a team of grant experts. Whether you're just starting your project or need to add the final touches to an application, their grant consultants have teamed up with Motorola Solutions to provide grant resources and services specific to communications. They do not guarantee funding but will do everything they can to assist you in submitting a successful grant application.
- **Application Deadline**: Ongoing
- **Website**: https://www.educationgrantshelp.com/motorola-edugh-grant-assistance/?elqTrackId=3aae997964b54dc8a5d0deabf807d032&elqaid=5675&elqat=2

Cyber Grants

- **Organization**: Motorola Solutions
- **Description**: Fill out the form online for customized grant assistance for projects in the Communications category for education. This includes grant research, grant alert notices, and grant application reviews from a team of grant experts. Whether you're just starting your project or need to add the final touches to an application, their grant consultants have teamed up with Motorola Solutions to provide grant resources and services specific to communications. They do not guarantee funding but will do everything they can to assist you in submitting a successful grant application.