Hazard Mitigation Activities under BRIC and FMA may Incorporate Cybersecurity Activities

This Program Support Material (PSM) provides information about the hazard mitigation activities eligible under the Building Resilient Infrastructure and Communities (BRIC) and Flood Mitigation Assistance (FMA) grant programs, and how to incorporate cybersecurity activities for the fiscal year 2022.

Background

Infrastructure is highly interconnected and can be vulnerable to evolving threats, particularly as it is modernized. Natural hazards can damage infrastructure and systems that rely on and support cybersecurity, and communities are more vulnerable to cyberattacks during disasters. These critical systems can be found in many types of public facilities, including hospitals, fire stations, emergency operations centers, evacuation shelters, public transportation, drinking water systems, wastewater treatment plants, and power generation facilities.

Further disruption to operating systems of critical infrastructure (including cybersecurity systems designed to protect that infrastructure) could have cascading impacts across and beyond a community. Hazard mitigation projects that incorporate eligible cybersecurity activities provide additional protection to critical infrastructure. Protection of the systems that keep infrastructure operating is becoming particularly important as cyberattacks and chances of damage from natural events to cyber or information technology (IT) infrastructure are increasing.

An increasingly digital world requires communities to develop comprehensive actions to address physical and cyber resilience. State, local, tribal and territorial (SLTT) governments should develop IT infrastructure that addresses current needs including protecting, interpreting and acting on cybersecurity information. FEMA understands these challenges and will fund eligible hazard mitigation projects that have a cybersecurity subcomponent.

The Fiscal Year (FY) 2022 BRIC and FMA Notices of Funding Opportunity (NOFOs) include provisions reinforcing that cybersecurity is part of the mitigation strategies that increase community resilience. BRIC and FMA awards cannot fund a stand-alone cybersecurity project. An eligible cybersecurity activity must serve as a functional component of an eligible mitigation activity and otherwise meet all applicable programmatic requirements.

FEMA works closely with the Cybersecurity and Infrastructure Security Agency (CISA) to ensure cybersecurity response plans are developed and coordinated by government and private-sector partners. FEMA is committed to promoting and sustaining a ready FEMA and prepared nation through the 2022–2026 FEMA Strategic Plan that includes posturing our nation to meet current and emerging threats, such as cybersecurity concerns.

FEMA

Eligible Cybersecurity Activities

The BRIC and FMA grant programs provide funds for projects that reduce or eliminate risks to people and property from natural hazards. For the FY22 BRIC and FMA grant cycles, FEMA can fund projects that include a cybersecurity subcomponent. Please refer to the BRIC or FMA FY22 NOFOs for the specific language regarding cybersecurity eligibility.

FEMA may fund hazard mitigation projects that include certain cybersecurity activities if the project will improve a community's resilience to natural hazards or ensure the continued operation of critical infrastructure. Eligible cybersecurity activities generally fall into one of three major categories: buildings, systems, or plans. To meet BRIC and FMA requirements, sub-applications that include cybersecurity components must list all eligible costs in the Benefit-Cost Analysis (BCA).

Activities Eligible Under BRIC

The BRIC program provides an opportunity to ensure the resilience of IT systems for cybersecurity while protecting critical physical infrastructure. Electronic data is essential to the operation of many public facilities and should be viewed as critical to the function of a facility as much as the power or water needed to keep the facility running. FEMA recognizes that resilience applies to continued access to this data, and that damaged physical systems and cyber data must be recovered quickly and efficiently to ensure minimal disruption.

Under BRIC, hazard mitigation projects that include a cybersecurity subcomponent are eligible in the BRIC State/Territory Allocation, Tribal Set Aside, and National Competition. Projects that are submitted for funding under BRIC's national competition will be scored using Qualitative Evaluation Criterion 1: Risk Reduction/Resilience Effectiveness (please refer to the Qualitative Evaluation Criteria section found in the FY22 BRIC NOFO). All cybersecurity activities should be identified in a local hazard mitigation plan. Sub-applicants and applicants must indicate in their applications how a proposed cybersecurity activity improves a community's resilience to natural hazards. A stand-alone cybersecurity project is not an eligible mitigation activity under BRIC or FMA.

The following is a non-exhaustive list of potential eligible cybersecurity activities that may be eligible for BRIC funding if incorporated into a hazard mitigation project:

- Cybersecurity activities for buildings:
    - Harden facilities (buildings, wiring, rooms) that house the cybersecurity system component such as computers, hardware, or the system's servers. This could also include elevation of server racks or physical components to mitigate damage in the event of a flood, similar to the elevation of power generation equipment.
    - Backup equipment installation to provide redundancies in IT systems for critical infrastructure; this may include equipment installation elsewhere on the property that would be less likely to be damaged in the event of a disaster.
    - Update wiring and other electrical components to ensure that older or substandard wiring does not cause loss of function or data in the event of a disaster or emergency.

  - Redundancy for necessary utilities (such as water for cooling) to ensure continuous operations.

- Cybersecurity activities for systems (hardware and software):

  - Critical IT system updates for enhanced cybersecurity, including the replacement of old/outdated computer equipment, the continued usage of which is susceptible to cyberattacks or external damage. Systems that use hard-to-obtain critical components may be converted, or modernized, to a standard as published by CISA (or another federal agency) that would prevent misuse or reduce the possibility of a cyberattack.

  - Ensure that software required for facility operations is up to date, prioritizing updates that address known exploited vulnerabilities. This could include software such as building management software that controls climate, power or other critical building functions, that if damaged or comprised would result in the loss of function of the facility or its services. If using this type of critical infrastructure control systems or operational technology, conduct a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable or untrusted.

  - Conduct a review to confirm that the facility or organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated. Purchase and installation of software used to validate that all remote access to the organization's network and privileged or administrative access requires multi- factor authentication to reduce the opportunity for system intrusions or cyberattacks.

  - Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure that backups are isolated from network connections.

- Cybersecurity plan:

  - Development of an applicant-level cybersecurity plan, based on CISA's *Cyber Guidance for Small Business*, may be eligible under the Capability- and Capacity-Building category. However, to be eligible, the cybersecurity plan must be developed and incorporated into the actions of a hazard mitigation plan, so this activity would be funded as part of an approved update to a hazard mitigation plan.

Activities Eligible under FMA

Under FMA, cybersecurity activities are allowable when included as a functional component of an eligible mitigation activity. To be eligible for funding, the project must reduce or eliminate the risk of repetitive flood damage to buildings insured under the National Flood Insurance Program (NFIP). A stand-alone cybersecurity project that does not act as a functional component of an eligible mitigation activity that reduces or eliminates the risk of repetitive flood damage will be determined ineligible.

The following is a non-exhaustive list of potential eligible FMA mitigation activities that may have a cybersecurity component:

- Projects that include flood mitigation of buildings containing cybersecurity/IT components if the project reduces the cost to the NFIP;

- Floodproofing non-residential buildings housing cybersecurity/IT components; and
- Upgrading IT system protection against floodwaters.

Information and Resources

BRIC and FMA program information is available on the FEMA BRIC webpage and the FEMA FMA webpage. The resources below provide additional information on cybersecurity grant programs.

If you are interested in applying for a CISA Cybersecurity grant, please review the FY 22 CISA NOFO which outlines the program eligibility requirements.

Under the Infrastructure Investment and Jobs Act (IIJA), also known as the Bipartisan Infrastructure Law, funding for standalone cybersecurity activities has been made available through other DHS grants, including:

- State and Local Cybersecurity Grant Program (SLCGP) and Tribal Cybersecurity Grant Program (TCGP): Funding from the State and Local Cybersecurity Grant Program (SLCGP) and the Tribal Cybersecurity Grant Program (TCGP) helps eligible entities address cybersecurity risks and threats to information systems owned or operated by—or on behalf of—state, local and territorial (SLLT) governments.

The following sites provide additional information about cybersecurity and cybersecurity grants:

- CISA: https://www.cisa.gov/
- Free cybersecurity tools and services: https://www.cisa.gov/free-cybersecurity-services-and-tools
- Homeland Security Grant Program: https://www.fema.gov/grants/preparedness/homeland-security
- Emergency Management Performance Grant Program: https://www.fema.gov/grants/preparedness/emergency-management-performance
- Transit Security Grant Program: https://www.fema.gov/grants/preparedness/transit-security
- Tribal Homeland Security Grant Program: https://www.fema.gov/grants/preparedness/tribal-homeland-security
- Port Security Grant Program: https://www.fema.gov/grants/preparedness/port-security

CISA Cybersecurity Resources: This list provides additional resources, not covered by the grant programs above, and recommended by CISA for communities considering cyber project subapplications to review.

- Cyber Resource Hub | CISA
- August 2022 Community Bulletin.pdf (cisa.gov)
- CyberGrants | CISA
- Publications Library | CISA
- CISA Services Catalog | CISA
- Free Cybersecurity Services and Tools | CISA
- Protecting Critical Infrastructure | CISA
- Regional Resiliency Assessment Program | CISA
- Methodology for Assessing Regional Infrastructure Resilience - Lessons Learned from the Regional Resiliency Assessment Program June 2021 (cisa.gov)
- Methodology for Assessing Regional Resilience (cisa.gov)