NATIONAL PRIORITY PROJECT IDEAS

As released from FEMA on 4/4/2020

SOFT TARGETS/CROWDED PLACES:

- Operational overtime
- Physical security enhancements
- Closed-circuit television security cameras
- Security screening equipment for people and baggage
- Lighting
- Access controls
- Fencing, gates, barriers, etc.

INFORMATION AND INTELLIGENCE SHARING:

- Fusion center operations
- Information sharing with all DHS components; fusion centers; other operational, investigative and analytic entities; and other federal law enforcement and intelligence entities
- Cooperation with DHS officials and other entities designated by DHS in intelligence, threat recognition, assessment, analysis and mitigation
- Identification, assessment and reporting of threats of violence
- Joint intelligence analysis training and planning with DHS officials and other entities designated by DHS

DOMESTIC VIOLENT EXTREMISM:

- Open-source analysis of misinformation campaigns, targeted violence and threats to life, including tips/leads and online/social media-based threats
- Sharing and leveraging intelligence and information, including open-source analysis
- Execution and management of threat assessment programs to identify, evaluate and analyze indicators and behaviors indicative of domestic violent extremists
- Training and awareness programs (e.g., through social media, suspicious activity reporting indicators and behaviors) to help prevent radicalization
- Training and awareness programs (e.g., through social media, suspicious activity reporting indicators and behaviors) to educate the public on misinformation campaigns

and resources to help them identify and report potential instances of domestic violent extremism\

COMMUNITY PREPAREDNESS AND RESILIENCE:

- Establish, train and maintain Community Emergency Response Teams (CERT) and Teen CERT, with a focus on historically underserved communities, including procurement of appropriate tools, equipment and training aides
- Local delivery of CERT train-the-trainer and CERT Program Manager courses to build local program training and maintenance capacity
- Provide continuity training, such as FEMA's Organizations Preparing for Emergency Needs training, to faith-based organizations, local businesses and community-based organizations such as homeless shelters, food pantries, nonprofit medical providers and senior care facilities to bolster their resilience to all hazards
- Partner with local school districts to deliver the Student Tools for Emergency Planning curriculum or other educational programming to guide students on how to create emergency kits and family communications plans
- Partner with key stakeholders to assist with completing the Emergency Financial First Aid Kit or a similar tool to bolster the disaster centric financial resilience of individuals and households
- Execute You are the Help Until the Help Arrives workshops in concert with community-based organizations to bolster individual preparedness
- Target youth preparedness using FEMA programing such as Prepare with Pedro resources and Ready2Help
- Promote community planning, coordination and integration of children's needs during emergencies through workshops like FEMA's Integrating the Needs of Children Community Mapping: identify community resources and characteristics in order to identify gaps in resources, identify hazards and vulnerabilities and inform action to promote resilience

CYBERSECURITY:

- Cybersecurity risk assessments
- Migrating online services to the ".gov" internet domain
- Projects that address vulnerabilities identified in cybersecurity risk assessments
    - Improving cybersecurity of critical infrastructure to meet minimum levels identified by the Cybersecurity and Infrastructure Security Agency
    - Cybersecurity training and planning

ELECTION SECURITY:

- Physical security planning support

- Physical/site security measures – e.g., locks, shatter proof glass, alarms, etc.
- General election security navigator support
- Cyber navigator support
- Cybersecurity risk assessments, training and planning
- Projects that address vulnerabilities identified in cybersecurity risk assessments
- Iterative backups, encrypted backups, network segmentation, software to monitor/scan and endpoint protection
- Distributed Denial of Service protection
- Migrating online services to the ".gov" internet domain