CISA
CYBER+INFRASTRUCTURE

February 18, 2020

CISA INSIGHTS

FY20 Preparedness Grant Guidance on Cyber, Soft Target, and Elections Security Investments

The Secretary of Homeland Security has released the Fiscal Year (FY) 2020 Preparedness Grant guidance. It directs and encourages investment in the areas of cybersecurity, soft targets and crowded places, intelligence and information sharing, emerging threats, and elections infrastructure security. These articulated priorities reflect the transformation underway in our shared risk environment and threat landscape. As a Nation with increasing reliance on collective preparedness and response, multi-disciplinary collaboration, and shared skills and resources, we must stay ahead of our adversaries. The challenges confronting State, Local, Tribal, and Territorial jurisdictions should and do inform how we prevent, prepare, protect, and respond to all-hazard situations, as well as domain-specific security conditions. The changes in the FY20 grant guidance reflect great opportunity for addressing emergent risks, closing historically underinvested capability and capacity gaps, and providing investment for high-performance innovations.

As the Nation's risk advisor, the Cybersecurity and Infrastructure Security Agency (CISA)—in collaboration with industry and government partners—helps organizations understand, reduce, and mitigate the risk of nation-state and non-state actors' malicious activity. CISA is providing recommendations to help partners frame the FY20 Preparedness Grant opportunities as a further means to remain vigilant and protected against potential cyber and physical threats.

The following considerations assist in answering the questions: How should I think about these investments and set priorities? Where does CISA see the greatest areas of risk-based investment need? Where can I find resources to consult, and get assistance in shaping investment justifications? Understanding that this is a long-term process, CISA plans to work closely with the Federal Emergency Management Agency, and you as our partner, on these new investment priorities—helping you beyond FY20 with technical assistance and other support.

PLANNING CONSIDERATIONS

Cybersecurity

As the dependence on and vulnerabilities to information technologies continue to expand, State, Local, Tribal, and Territorial agencies must keep pace by deploying consensus cybersecurity best practices. Involve Chief Information Officers and Chief Information Security Officers as you consider the following:

- **Fundamentals.** Focus on training staff, understanding who is and what is on your networks, protecting your data, and planning for resiliency, including cyber incident response plans at state and local levels.
- **Investment.** Invest in transparent, enterprise-wide capabilities that minimize attack surface, disrupt malicious connections, and ensure recoverability of normal operations.
- **Holistic View.** Take regional or state-wide approaches, increasing effectiveness and efficiency.

Soft Targets and Crowded Places

Sports venues, shopping venues, schools, transportation systems, as well as other soft targets and crowded places are easily accessible to large numbers of individuals and often have limited security or protective measures in place. State, Local, Tribal, and Territorial agencies should consider focusing their investments in the following areas:

- **Plan.** Prepare government, businesses, and the public to prevent attacks on soft targets.
- **Train.** Identify and report suspicious behavior so it can be addressed.
- **Protect.** Protect against acts of violence and unmanned aircraft systems.
- **Prepare.** Prepare and respond to active assailants and bombings.

Election Security

When allocating resources to assist in election security, state and local jurisdictions are encouraged to follow guidance from their state election officials, the Election Assistance Commission, CISA's Election Security Resource Guide, and the Election Infrastructure Government Coordinating Council Funding Considerations document. This guidance includes:

- **Plan.** Establish processes and implement best practices to add resilience to America's elections.
- **Prepare.** Train and exercise to ensure everyone understands their role in election security.
- **Invest.** Invest in systems and associated security controls specific to election infrastructure.

INVESTMENT CONSIDERATIONS

Cybersecurity

- **Investment in Network Architecture and Cybersecurity Assessments.** A full system architecture review can be a critical starting point for risk mitigation decisions. Findings should drive future investments.
- **Data Protection, Backup, and Recovery.** Consider investing in technologies to protect data critical to your agency's mission, to include voter registration databases. Also consider capabilities that automatically and continuously back up your business-critical data and system configurations as they change.
- **DNS Filtering Services.** Sometimes referred to as Domain Name Service Blocking or Firewall, consider DNS filtering services with integrated threat intelligence to filter and prevent establishment of connections to unauthorized websites, suspicious domain names, and known malicious domain names associated with malware and phishing.
- **Patch and Update Management.** Consider capabilities that keep you aware of the status of assets and shorten the time needed to obtain and deploy software and firmware patches.
- **Application to Emergency Communications.** Apply best practices to the protection of Public Safety Answering Points; include foundational cybersecurity measures as part of a transition to Internet Protocol-based networks supporting Next Generation 9-1-1.
- **DMARC.** Domain-based Message Authentication, Reporting, and Conformance is an email authentication protocol that protects again email spoofing.
- **Training and Exercises.** Train staff to reduce susceptibility to phishing attacks, promote general cybersecurity awareness, and conduct table top exercises to improve resilience.
- **Get on DotGov.** The .gov top-level domain is a more secure environment for bona fide U.S.-based State, Local, Tribal, and Territorial government organizations.
- **Building Cyber Liaison Programs.** Establish liaisons, or "navigators," to provide practical cybersecurity knowledge, support, and services to State, Local, Tribal, and Territorial agencies and local election officials

Note: *Many of the cybersecurity-focused investment considerations outlined above will also provide security and resilience benefits for election infrastructure.*

Soft Targets and Crowded Places

Based on the Securing Soft Targets and Crowded Places Resource Guide, investments to consider include:

- **Assessment Teams.** Develop assessment teams, to include security planning activities and training.
- **Risk Management.** Assess critical sites, such as schools, polling and caucus locations, and other public venues.
- **Training and Exercises.** Train staff and participate in tabletop exercises and drills to prepare for safety incidents.
- **Implement Best Practices.** Incorporate assessment results into emergency operations plans.

State, Local, Tribal, and Territorial agencies should also consider how investments within the grant guidance can improve school safety. Resources to support threat assessment, emergency operations planning, and training and exercises to promote safer and more resilient schools can be found at Schoolsafety.gov.

ADDITIONAL INFORMATION

To engage with CISA Regional personnel is in your area of operation, please contact the CISA at cisaservicedesk@cisa.dhs.gov. CISA operates ten (10) Regional offices that provide stakeholder services and resources that can help shape investment justifications. Some of options and considerations may be long-term in nature. Early engagement with regional personnel who live and work in your communities will allow for more effective security planning for your specific organization.

For more information visit CISA.gov