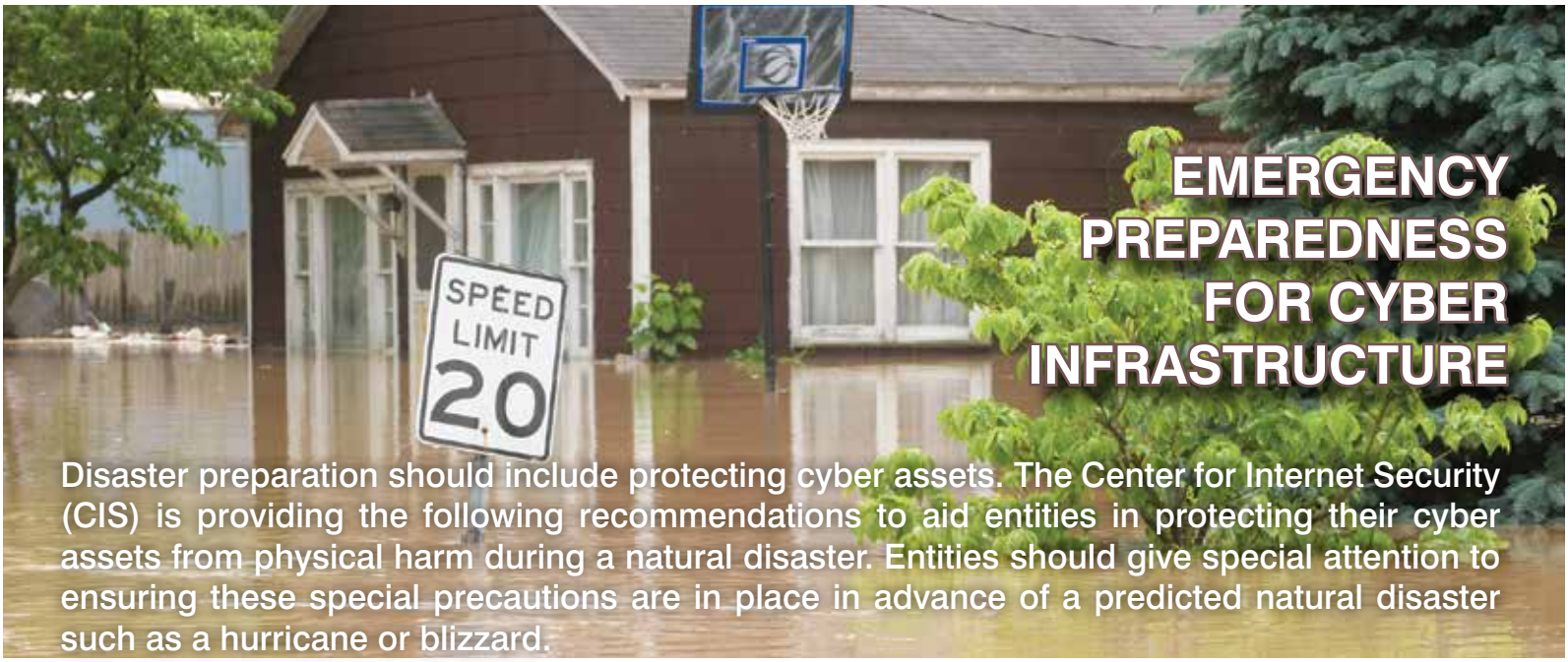

EMERGENCY PREPAREDNESS FOR CYBER INFRASTRUCTURE

Disaster preparation should include protecting cyber assets. The Center for Internet Security (CIS) is providing the following recommendations to aid entities in protecting their cyber assets from physical harm during a natural disaster. Entities should give special attention to ensuring these special precautions are in place in advance of a predicted natural disaster such as a hurricane or blizzard.

Technical Recommendations:

• Run a full backup on all servers and test installing backups on a clean machine to ensure that reinstallation can occur. Store copies of all items necessary to perform fresh installations, such as backups, configuration files, cabling, media, serial numbers, and license keys at a secure, off-site location. If possible, store spare equipment at an off-site location.

• Test all emergency operations plans, especially plans that include equipment failure and relocation. Ensure that information technology staff are included in emergency preparations and are available for immediate response; do not assume that staff will have remote access capabilities. Ensure that all remote staff are informed of network changes during preparation.

• Know what cyber infrastructure is required for key tasks and where it is physically located. Cyber infrastructure may include communications infrastructure provided by a third party, and key databases and software for first responders, incident coordinators, and emergency managers.

• Consider the possible results of damage to structures, such as flooding and broken windows. If equipment can be moved permanently or in advance of a predicted event, do so; ideally sensitive equipment should be in an interior room, above ground level, away from windows, and off the floor.

• Ensure redundant infrastructure, including alternative power sources, is tested and operational. When possible, have surplus and back-up equipment, including power cords, cables, and fans for cooling a server room, stored in locations where they are easily accessible. If it is common to lose power, consider supplementing battery power with extended-life chargers and/or solar chargers.

• If there are single points-of-failure, such as communication towers/antennas or fiber paths along bridges/tunnels, consider response plans for repairing those crucial protection/recovery points.

• Review access control measures and restrictions to ensure that essential employees can still gain access to critical locations in the event of a power failure or if computer networks are offline.

• Have contingency plans in place in case of infrastructure failures and train users in how to complete essential tasks without telephones, Internet connectivity, and computers.

• Where possible, ensure all battery operated electronic devices are charged and unplugged.

• Encrypt or password protect all electronic devices in case of evacuation.

• If appropriate, have pre-established agreements with vendors to ensure replacement equipment and software is available on a priority basis, and through a line of credit, if needed.

• Ensure that up-to-date equipment insurance policies provide sufficient coverage.

Keep a hard copy list of critical information, including:

• Emergency contacts and information for essential equipment/software/vendors and department employees, including special escalation procedures for natural disasters. Test the list regularly.

• Additional items necessary for a support call, such as contact numbers, support numbers, license keys and serial numbers, and exact configuration settings (hardware requirements, drive letters and sizes, patches, hot fixes, etc.) and restoration instructions.

For more information regarding this cyber threat, please contact: Multi-State Information Sharing and Analysis Center, 31 Tech Valley Drive East Greenbush, NY 12064; Ph: (866) 787-4722; email: SOC@cisecurity.org; www.cisecurity.org.