1. Block all international internet access. Build a USA perimeter screening which basically means anything traversing across in and out to a foreign government- friend or foe- will be blocked until critical business head approves. Includes gmail, facebook, $$ transfers, all protocols, etc. Users who have legitimate business overseas by Internet must register with Homeland Security when critical infrastructure identified with continued Internet access allowed. Internal and external monitoring must be implemented.

2. Properly vet foreign students / foreign visitors/ green card prior to allowing USA internet access. Have each sign a non-abuse USA internet policy, USA PII usage, identity theft prevention, etc. Prevent USA citizens found to violate USA internet policy from having access. Treat illegal internet users as criminals - both US citizen and non- US citizen. Have internet service providers on-board. Define illegal internet use.

3. Completely isolate critical infrastructures from Internet access. No public IP addresses and no Internet. All updates to critical infrastructure will be manual mode by vetted personnel. Updates will be tested prior to updating production systems.

4. All critical infrastructures must be encrypted to the current FIPS methodology. Infrastructure must use it's independently owned fiber connectivity.

5. Do not allow any backups or storage in the cloud of critical infrastructure data.

6. Do not allow virtualization of any critical infrastructures. Make sure each run in their own instance with appropriate patches, antivirus.

7. Do not allow personally owned devices nor remote access into critical infrastructures.

8. Ensure there are appropriate vetted personnel who know how to detect, monitor, take corrective action, document security incidents, etc to protect the critical infrastructures.

9. Do not allow critical infrastructures as world wide web access. With internet access are risks. If risk is taken, must be able to monitor, detect and eradicate any issues- being proactive instead of only reactive. Must limit access to within the US and must be able to validate end user by using computer 2 factor authentication and a second authorized person must also sign-off as allowing. If both are not completed, access is denied and the computer requesting remote access will be blocked until legitimately authorized by second person. 2 factor authentication and 2 people authentication. All of these events must be logged.