The White House Urges Companies to Take These Steps Immediately:

1. MANDATE the use of multi-factor authentication on your systems to make it harder for attackers to get into your system

2. DEPLOY modern security tools on your computers and devices to continuously look for and mitigate threats

3. CHECK with your cybersecurity professionals to make sure that your systems are patched and protected against all known vulnerabilities, and change passwords across your networks so that previously stolen credentials are useless to malicious actors

4. BACK UP YOUR DATA and ensure you have offline backups beyond the reach of malicious actors

5. RUN EXERCISES and drill your emergency plans so that you are prepared to respond quickly to minimize the impact of any attack

6. ENCRYPT your data so it cannot be used if it is stolen

7. EDUCATE your employees to common tactics that attackers will use over email or through websites, and encourage them to report if their computers or phones have shown unusual behavior, such as unusual crashes or operating very slowly

8. ENGAGE PROACTIVELY with your local FBI field office or CISA Regional Office to establish relationships in advance of any cyber incidents. Please encourage your IT and Security leadership to visit the websites of CISA and the FBI, where they will find technical information and other useful resources.