Floating Pragma

Description

Contracts should be deployed with the same compiler version and flags that they have been tested with thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively.

Remediation

Lock the pragma version and also consider known bugs (https://github.com/ethereum/solidity/releases) for the compiler version that is chosen.

Pragma statements can be allowed to float when a contract is intended for consumption by other developers, as in the case with contracts in a library or EthPM package. Otherwise, the developer would need to manually update the pragma in order to compile locally.

Example:

Code:

```
1 pragma solidity ^0.4.0;
2
3 contract PragmaNotLocked {
4     uint public x = 1;
5 }
```
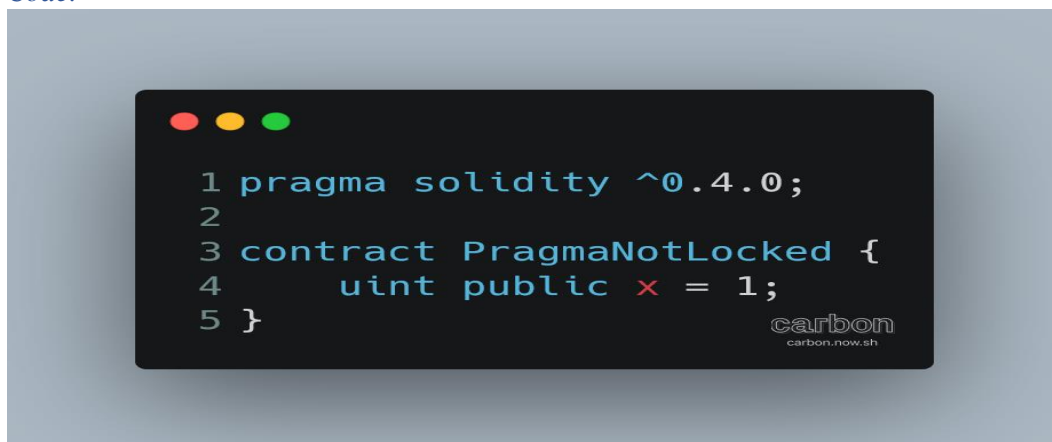
Explanation:

The best practice is to lock a pragma version and deploy the contract to the mainnet. Using different pragma versions in test and mainnet may introduce unknown security risks.

Example pragma code statement
pragma solidity >=0.4.0 < 0.6.0;
pragma solidity >=0.4.0<0.6.0;
pragma solidity >=0.4.14 <0.6.0;
pragma solidity >0.4.13 <0.6.0;
pragma solidity 0.4.24 - 0.5.2;