In contrast to its wired counterpart, wireless communication is highly susceptible to eavesdropping due to the broadcast nature of the wireless propagation medium. Recent works have proposed the use of interference to reduce eavesdropping capabilities in wireless wiretap networks. However, the concurrent effect of interference on both eavesdropping receivers (ERs) and legitimate receivers has not been thoroughly investigated, and careful engineering of the network interference is required to harness the full potential of interference for wireless secrecy. This two-part article addresses this issue by proposing a generalized interference alignment (GIA) technique, which jointly designs the transceivers at the legitimate partners to impede the ERs without interfering with LRs. In Part I, we have established a theoretical framework for the GIA technique. In Part II, we will first propose an efficient GIA algorithm that is applicable to large-scale networks and then evaluate the performance of this algorithm in stochastic wireless wiretap network via both analysis and simulation. These results reveal insights into when and how GIA contributes to wireless secrecy.