

OFF TO A FAST START

In addition to the near-daily reports of more breaches, new laws and controversial workplace privacy issues, there have been 3 significant developments involving cyber and privacy already in 2013.

1. On January 17, 2013 the Department of Health and Human Services released its final “omnibus” rule in relation to HIPAA, effective March 26, 2013. The sweeping rule implements privacy regulations, increases penalties for HITECH violations, modifies breach notification rules, restricts disclosure of genetic information and expands the definition and responsibilities of business associates.
2. In his State of the Union address on February 14, 2013 President Obama unveiled an Executive Order on Cybersecurity. An executive order does not carry the same effect of law, and it mostly encourages voluntary conduct among federal agencies and the private sector. But the order raises awareness of threats to critical infrastructures, balanced against the preservation of privacy and civil liberties.
3. On February 17, 2013 Mandiant, a US security company, released a report detailing massive espionage into US companies by hackers associated with the Chinese military under the mysterious name “Unit 61398.” The scope and pervasiveness of this type of hacking reminds all businesses that they must take cyber threats seriously and implement preventative measures. Because the risk is not only to third parties but also to their intellectual property.

[Click here](#) to visit the CyBIR blog and read additional cyber articles.