Bloomberg BNA

Privacy Law Watch Bulletin™

VOL. 17, NO. 4 JANUARY 6, 2017

*Cybersecurity*

## Companies Should Help Fight Foreign Cybersecurity Threats, Intel Chiefs Say

U.S. companies shouldn't wait for Congress before taking action to address cybersecurity, top intelligence officials said at a Jan. 5 Senate hearing.

Cybersecurity threats are real and demand immediate attention from companies as well as the federal government, Director of National Intelligence James R. Clapper Jr.; Under Secretary of Defense for Intelligence Marcel J. Lettre II; and Chief of U.S. Cyber Command, Director of the National Security Agency and Chief of Central Security Services Michael S. Rogers told the Senate Armed Services Committee.

The focus of the U.S. Senate Committee on Armed Services hearing was mainly around Russia's alleged involvement in hacks that attempted to sway the 2016 presidential election. Immediately after the hearing, panel Chairman John McCain (R-Ariz.) told reporters that in a broad sense the Russian intrusions were an ''act of war.''

The intelligence officials said private-public partnerships to address cybersecurity are essential.

Laura E. Jehl, partner at Sheppard, Mullin, Richter & Hampton LLP in Washington and co-leader of the firm's Privacy and Cybersecurity Practice, told Bloomberg BNA Jan. 5 that although companies shouldn't rely on the U.S. government for cybersecurity preparedness, ''there's a role for public private partnerships.'' The recent Joint Analysis Report detailing tools allegedly used by the Russia government-sponsored hackers is a ''great example of private-public information sharing that benefits everyone.''

Rogers and Clapper expressed concerns over cybersecurity workforce issues, saying that the lack of a high-end professionals may be hurting U.S. cybersecurity preparedness in both the public and private sectors.

**Private-Public Partnerships** Even with the loss of some of the cybersecurity workforce to the private sector, the government should still share information with the private sector to help combat foreign cyberattacks.

A hallmark of private-public partnerships is cybersecurity information sharing programs, which the U.S. implemented in December 2015 as part of the Cybersecurity Information Sharing Act (CISA). CISA protects companies that share cybersecurity threat indicators or defensive measures with the government. Under CISA, private entities that ''promptly'' share their data with the government are granted immunity from any public or private cause of action.

Kendall C. Burman, cybersecurity and data privacy counsel at Mayer Brown LLP in Washington, told Bloomberg BNA Jan. 5 that private-public partnerships ''and information sharing are pieces'' of the cybersecurity puzzle. There's no ''question that the private sector must lean forward on cybersecurity and that the government has a critical role as well,'' she said.

The important question going forward is how the U.S. government and private industry ''can work together to be most effective and what needs to happen to better understand their respective roles'' in cybersecurity preparedness, detection and prevention, Burman, who previously served in the Obama administration, said.

Bill Wright, director of government affairs and senior policy counsel at cybersecurity company Symantec Corp, told Bloomberg BNA Jan. 5 that private-public partnerships and information sharing are helpful to stop foreign cyberattacks, but raised concern that some companies may rely on congressional action for assistance. While assistance may be helpful, especially for small businesses, companies shouldn't ''rely entirely on the government because no government in this world can completely stop this threat,'' he said.

If there is a ''silver bullet to cybersecurity'' it will probably come from private-public partnerships, Wright said.

**Cybersecurity Staffing Concerns** Recent statements made by the Trump administration disparaging the intelligence community's report on the alleged Russian hacking may be hurting the U.S.'s ability to hire a competent cybersecurity workforce.

Rogers said at the hearing that private and public sectors need enhancements to the cybersecurity workforce. Clapper also raised concerns that Trump's statements about the U.S. intelligence community is leading to the ''high-end cybersecurity workforce'' leaving the government for the private sector.

Wright said that the U.S. government has been doing a better job ''over the last year or so to sweeten the pot'' to attract cybersecurity professionals. Hopefully the government can fill these roles to better enhance government cybersecurity protection.

Jehl agreed that the government's cybersecurity outlook isn't as bleak as Rogers and Clapper made it seem. The U.S. has ''has tremendous resources which can be brought to bear to identify the source of cyberattacks and to educate others who may be at risk,'' she said. This is beneficial to both the private and public sectors, she said.

By Daniel R. Stoller

 ISSN 0000-0000

To contact the reporter on this story: Daniel R. Stoller in Washington at dstoller@bna.com

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com

*Further information on the hearing is available at http://www.armed-services.senate.gov/hearings/17-01-05-foreign-cyber-threats-to-the-united-states.*

  PRA ISSN 0000-0000