

Sent: Mon, 08 Oct 2012 14:11:07 -0400
From: "ERIC ENGLEMAN (BLOOMBERG/ NEWSROOM:)" <eengleman1@bloomberg.net>
To: "Hayden, Caitlin" <caitlin_m_hayden@nss.eop.gov>, "Hayden, Caitlin" </o=eop/ou=exchange administrative group /cn=recipients/cn=caitlin_m_hayden">
Subject: Fwd:For Immediate Release--Chairman Rogers and Ranking Member Ruppertsberger Warn American Companies Doing Business with Huawei and ZTE to "use another vendor"
[alt_body.html](#)
[image003.png](#)

Caitlin, any White House reaction to this report from House Intelligence Committee today to Huawei/ZTE?

Thank you,
Eric Engleman
Bloomberg News

Eric Engleman
Technology Reporter
Bloomberg News, Washington Bureau
(o) (202) 624-1815
(m) [REDACTED] - - - - -
eengleman1@bloomberg.net
Twitter: @ericengleman

P6/b(6)

----- Original Message -----

From: Ashley.Lowry@mail.house.gov
To: ERIC ENGLEMAN (BLOOMBERG/ NEWSROOM:)
At: Oct 8 2012 10:16:20

[cid:image003.png@01CDA531.2C314760]

For Immediate Release Contact: Susan Phalen (Rogers)
October 8, 2012 Susan.Phalen@mail.house.gov<mailto:Susan.Phalen@mail.house.gov>
Heather Moeder Molino (Ruppertsberger)
Heather.Molino@mail.house.gov<mailto:Heather.Molino@mail.house.gov>

Chairman Rogers and Ranking Member Ruppertsberger Warn American Companies Doing Business with Huawei and ZTE to "use another vendor"

WASHINGTON, D.C. - The Chairman and Ranking Member of the House Intelligence Committee, Mike Rogers (R-MI) and C.A. Dutch Ruppertsberger (D-MD), today released a report recommending to U.S. companies considering doing business with Chinese telecommunications companies Huawei and ZTE to find another vendor. The report encourages U.S. companies to take into account the long-term security risks associated with either company providing equipment or services to our telecommunications infrastructure. Additionally, the report recommends that U.S. government systems, particularly sensitive systems, exclude Huawei or ZTE equipment or component parts.

The report highlights the interconnectivity of U.S. critical infrastructure systems and warns of the heightened threat of cyber espionage and predatory disruption or destruction of U.S. networks if telecommunications networks are built by companies with known ties to the Chinese state, a

country known to aggressively steal valuable trade secrets and other sensitive data from American companies.

Additionally, the report notes that modern critical infrastructure is incredibly connected, everything from electric power grids to banking and finance systems to natural gas, oil, and water systems to rail and shipping channels. All of these entities depend on computerized control systems. The risk is high that a failure or disruption in one system could have a devastating ripple effect throughout many aspects of modern American living.

The report, released today in a Capitol Hill news conference, states that Huawei and ZTE provided incomplete, contradictory, and evasive responses to the Committee's core concerns. The report comes after a year-long investigation into the national security dangers posed by Huawei and ZTE, the two largest Chinese telecommunications companies doing business in the United States.

The report includes five recommendations.

1. US government systems and US government contractors, particularly those working on sensitive systems, should exclude any Huawei or ZTE equipment or component parts. Additionally, the Committee on Foreign Investments in the United States (CFIUS) must block acquisitions, takeovers, or mergers involving Huawei and ZTE given the threat to U.S. national security interests.

1. U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects.

1. Unfair trade practices of the Chinese telecommunications sector should be investigated by committees of jurisdiction in U.S. Congress and enforcement agencies in the Executive Branch. Particular attention should be paid to China's continued financial support of key companies.

1. Chinese companies should quickly become more open and transparent. Huawei, in particular, must become more transparent and responsive to U.S. legal obligations.

1. Committees of jurisdiction in Congress should consider potential legislation to better address the risk posed by telecommunications companies with nation-state ties or otherwise not clearly trusted to build critical infrastructure, including increasing information-sharing among private sector entities and expanding a role for the CFIUS process to include purchasing agreements.

"We have to be certain that Chinese telecommunication companies working in the United States can be trusted with access to our critical infrastructure," Chairman Rogers said. "Any bug, beacon, or backdoor put into our critical systems could allow for a catastrophic and devastating domino effect of failures throughout our networks. As this report shows, we have serious concerns about Huawei and ZTE, and their connection to the communist government of China. China is known to be the major perpetrator of cyber espionage, and Huawei and ZTE failed to alleviate serious concerns throughout this important investigation. American businesses should use other vendors."

"It is our responsibility on the Intelligence Committee to protect our country's national security. That is why we launched this investigation in the first place. We depend on our nation's networks for so much of what we do every day. As this report shows, we have serious concerns about Huawei and ZTE, two Chinese telecommunications companies looking to gain market share in the United States, and their connection to the communist government of China. We warn U.S. government agencies and companies considering using Huawei and ZTE equipment in their

networks to take into account the affect if could have on our national security," said Ranking Member Ruppersberger.

History of the Investigation

In early 2011, shortly after becoming Chairman and Ranking Member of the House Intelligence Committee, Chairman Rogers and Ranking Member C.A. Dutch Ruppersberger instructed committee staff to conduct a preliminary review of the national security threats posed by Chinese telecom companies doing business in the United States. The preliminary review suggested that the threat to the supply chain constitutes a rising national security concern of the highest priority. Thus, on November 17, 2011, the House Intelligence Committee launched a full investigation, focusing on the two main Chinese telecommunication companies doing business in the United States, Huawei and ZTE.

The focus of the investigation was to review the history, management, and operations of key Chinese companies seeking to expand into U.S. infrastructure. The investigation reviewed the extent to which these companies have ties to the Chinese government and Chinese Communist Party, or otherwise provide the Chinese government greater opportunities for foreign and economic espionage.

In February and April 2012 HPSCI investigators traveled to China to interview officials at Huawei and ZTE headquarters. Then, in May 2012, several members of the committee, including Ranking Member Ruppersberger, traveled to Hong Kong to meet with senior officials from both Huawei and ZTE. In September 2012 the House Intelligence Committee held a rare open hearing, where officials of both Huawei and ZTE testified before Congress. That hearing marked the first time Chinese executives have testified before the U.S. Congress.

Link to the Full Report:

<http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf>

For Immediate Release
October 8, 2012

(Ruppersberger)

Contact: **Susan Phalen (Rogers)**
 Susan.Phalen@mail.house.gov
Heather Moeder Molino

Heather.Molino@mail.house.gov

Chairman Rogers and Ranking Member Ruppersberger Warn American Companies Doing Business with Huawei and ZTE to “use another vendor”

WASHINGTON, D.C. – The Chairman and Ranking Member of the House Intelligence Committee, Mike Rogers (R-MI) and C.A. Dutch Ruppersberger (D-MD), today released a report recommending to U.S. companies considering doing business with Chinese telecommunications companies Huawei and ZTE to find another vendor. The report encourages U.S. companies to take into account the long-term security risks associated with either company providing equipment or services to our telecommunications infrastructure. Additionally, the report recommends that U.S. government systems, particularly sensitive systems, exclude Huawei or ZTE equipment or component parts.

The report highlights the interconnectivity of U.S. critical infrastructure systems and warns of the heightened threat of cyber espionage and predatory disruption or destruction of U.S. networks if telecommunications networks are built by companies with known ties to the Chinese state, a country known to aggressively steal valuable trade secrets and other sensitive data from American companies.

Additionally, the report notes that modern critical infrastructure is incredibly connected, everything from electric power grids to banking and finance systems to natural gas, oil, and water systems to rail and shipping channels. All of these entities depend on computerized control systems. The risk is high that a failure or disruption in one system could have a devastating ripple effect throughout many aspects of modern American living.

The report, released today in a Capitol Hill news conference, states that Huawei and ZTE provided incomplete, contradictory, and evasive responses to the Committee’s core concerns. The report comes after a year-long investigation into the national security dangers posed by Huawei and ZTE, the two largest Chinese telecommunications companies doing business in the United States.

The report includes five recommendations.

1. US government systems and US government contractors, particularly those working on sensitive systems, should exclude any Huawei or ZTE equipment or component parts. Additionally, the Committee on Foreign Investments in the United States (CFIUS) must block acquisitions, takeovers, or mergers involving Huawei and ZTE given the threat to U.S. national security interests.
2. U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects.
3. Unfair trade practices of the Chinese telecommunications sector should be investigated by committees of

jurisdiction in U.S. Congress and enforcement agencies in the Executive Branch. Particular attention should be paid to China's continued financial support of key companies.

4. Chinese companies should quickly become more open and transparent. Huawei, in particular, must become more transparent and responsive to U.S. legal obligations.

5. Committees of jurisdiction in Congress should consider potential legislation to better address the risk posed by telecommunications companies with nation-state ties or otherwise not clearly trusted to build critical infrastructure, including increasing information-sharing among private sector entities and expanding a role for the CFIUS process to include purchasing agreements.

"We have to be certain that Chinese telecommunication companies working in the United States can be trusted with access to our critical infrastructure," Chairman Rogers said. "Any bug, beacon, or backdoor put into our critical systems could allow for a catastrophic and devastating domino effect of failures throughout our networks. As this report shows, we have serious concerns about Huawei and ZTE, and their connection to the communist government of China. China is known to be the major perpetrator of cyber espionage, and Huawei and ZTE failed to alleviate serious concerns throughout this important investigation. American businesses should use other vendors."

"It is our responsibility on the Intelligence Committee to protect our country's national security. That is why we launched this investigation in the first place. We depend on our nation's networks for so much of what we do every day. As this report shows, we have serious concerns about Huawei and ZTE, two Chinese telecommunications companies looking to gain market share in the United States, and their connection to the communist government of China. We warn U.S. government agencies and companies considering using Huawei and ZTE equipment in their networks to take into account the affect if could have on our national security," said Ranking Member Ruppertsberger.

History of the Investigation

In early 2011, shortly after becoming Chairman and Ranking Member of the House Intelligence Committee, Chairman Rogers and Ranking Member C.A. Dutch Ruppertsberger instructed committee staff to conduct a preliminary review of the national security threats posed by Chinese telecom companies doing business in the United States. The preliminary review suggested that the threat to the supply chain constitutes a rising national security concern of the highest priority. Thus, on November 17, 2011, the House Intelligence Committee launched a full investigation, focusing on the two main Chinese telecommunication companies doing business in the United States, Huawei and ZTE.

The focus of the investigation was to review the history, management, and operations of key Chinese companies seeking to expand into U.S. infrastructure. The investigation reviewed the extent to which these companies have ties to the Chinese government and Chinese Communist Party, or otherwise provide the Chinese government greater opportunities for foreign and economic espionage.

In February and April 2012 HPSCI investigators traveled to China to interview officials at Huawei and ZTE headquarters. Then, in May 2012, several members of the committee, including Ranking Member Ruppertsberger, traveled to Hong Kong to meet with senior officials from both Huawei and ZTE. In September 2012 the House Intelligence Committee held a rare open hearing, where officials of both Huawei and ZTE testified before Congress. That hearing marked the first time Chinese executives have testified before the U.S. Congress.

Link to the Full Report:

<http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf>

The background of the image is a stylized American flag. The stars and stripes are visible, with a large eagle in flight on the left side, its wings spread wide. The eagle is dark with a white head and neck.

U.S. House of Representatives

PERMANENT SELECT COMMITTEE ON

INTELLIGENCE