PETER T. KING, NEW YORK
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Twelfth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

December 16, 2011

The Honorable Caryn Wagner
Under Secretary for Intelligence and Analysis
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Under Secretary Wagner:

On October 31st at a session of the National Symposium on Homeland Security and Defense, you made comments indicating the Department of Homeland Security (DHS) is developing new guidelines for intelligence analysts to use while monitoring social media online.[1] We are writing to inquire about the progress DHS has made in developing these guidelines for the DHS Intelligence Enterprise, in particular the Office of Intelligence and Analysis (I&A), to collect open source intelligence on the Internet, including social networking websites such as Twitter and Facebook.

As you know, social media has increasingly been a crucial source of intelligence collection on significant world events. In 2011, protestors in various countries across the Middle East and North Africa used social networking to organize protests and report breaking developments. Senator Dianne Feinstein, Chairwoman of the Senate Select Committee on Intelligence, observed that the U.S. Intelligence Community missed the warning signs of widespread uprisings in countries such as Egypt, despite significant indications on social networking sites such as Twitter.[2] With nearly one billion Facebook users and hundreds of millions of Twitter postings every day, social media can provide numerous resources for identifying broad trends, popular sentiments, and breaking newsworthy events. We believe it would be advantageous for DHS and the broader Intelligence Community to carefully parse the massive streams of data from various social media outlets to identify current or emerging threats to our homeland security.

Although there are clear advantages to monitoring social media to identify possible threats to our security, there are also privacy and civil liberties concerns implicit in this activity. With its domestic mission, the Department of Homeland Security needs to be mindful of the rights of the citizens of our country to express themselves online. Not only should any guidance issued by the Department permit analysts to do their jobs identifying threats, but it should also be stringent enough to protect the rights of our citizens.

---

[1] "Department of Homeland Security to step up monitoring of Twitter and other social network sites," *Daily Mail UK.* November 1, 2011. Available at: http://www.dailymail.co.uk/news/article-2056140/Homeland-Security-step-monitoring-Twitter-social-network-sites.html

[2] "Dianne Feinstein: U.S. intel missed warnings in Egypt," *Politico,* February 16, 2011. Available at: http://www.politico.com/news/stories/0211/49686.html

Since open source intelligence collection is one of the only collection missions of the Office of Intelligence and Analysis, we believe it is critical that the Department issues guidelines to I&A analysts that allow the collection and analysis of information from social media websites to be an expanding and important competency of I&A. The Department should issue clear, effective guidance enabling the harnessing of this important information source while protecting privacy and civil liberties of U.S. citizens.

Therefore, pursuant to Rule X (3)(g) and Rule XI of the Rules of the House of Representatives, please provide the information requested below, in writing and in classified and unclassified format, as appropriate, no later than February 15, 2011:

1. When will the guidelines on the use of social media for intelligence purposes be issued to the Department? Prior to this new set of guidelines, what previous guidelines were intelligence analysts operating under when monitoring social media websites? Who are the principle DHS officials involved in the drafting of this guidance? Will there be one uniform set of guidelines Department-wide, or will the guidelines only be applicable to the DHS Intelligence Enterprise or DHS members of the Intelligence Community? If and/or when they are available, please provide copies of all pertinent, current, written guidelines to the Subcommittee.

2. How will the guidelines take privacy and civil liberties of U.S. persons into account? Have there been any Privacy Impact Assessments or other assessments conducted on the collection of information from social media sites? If so, please provide the Subcommittee with copies of the assessments.

3. What technologies does DHS leverage to ingest the massive amount of data from the Internet to analyze broad trends? Does DHS need more research and development in this area?

4. Is there a strategic plan for expanding or evolving the DHS Open Source Enterprise to better take advantage of social media? Do you anticipate a larger budget request in this area for FY 2013? How many I&A analysts are currently dedicated to open source intelligence collection and analysis? Please state how many of these analysts are government employees and how many are contractors.

5. When conducting open source intelligence training for DHS and state and local fusion center analysts, is there guidance specific to social media included in the program?

6. How does DHS ensure specialized training for social media analysis? For example, as you know, traditional sources of intelligence such as human intelligence (HUMINT) are vetted to determine source credibility and reliability over a period of time. Social media lends itself to a great deal of misinformation and disinformation, both of which significantly impacts the end product if not correctly identified. How will DHS ensure its analysts are fully equipped to handle this task?

7. What are the authorities and restrictions for the DHS Open Source Enterprise collection activities? Do you believe any new authorities are necessary to enhance this mission?

8. What is the relationship between the DHS Open Source Enterprise and the Office of the Director of National Intelligence's Open Source Center (OSC)? Does DHS leverage OSC materials, and are DHS open source products available at OSC?

Thank you for your attention to this matter. If you have any questions about this request, please contact us at (202) 226-8417 or (202) 226-2616.

Sincerely,

PATRICK MEEHAN
Chairman
Subcommittee on Counterterrorism
and Intelligence

JACKIE SPEIER
Ranking Member
Subcommittee on Counterterrorism
and Intelligence