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

July 25, 2012

The Honorable John S. Pistole
Administrator
Transportation Security Administration
601 S. 12th Street
Arlington, VA 20528

Dear Administrator Pistole:

We write to you seeking further clarification on the Transportation Security Administration's (TSA) June 20, 2012 posting on the Federal Business Opportunities Website, titled "Insider Threat Software."[1]

On June 25, 2012, we wrote to you requesting that TSA cease its efforts to acquire "Insider Threat Software." TSA's response clarified that the notice contained on the Federal Business Opportunities Website was not a solicitation but was "an informal market research technique, commonly employed prior to a formal acquisition."[2] While the clarification is appreciated, it fails to address the issues raised in the letter.

As TSA proceeds with its efforts to acquire this software, we continue to have questions regarding both the need to acquire this type of software and its expected scope of use. Further, we continue to have questions regarding any processes, which will be implemented by TSA to ensure use of the software is in accordance with the Office of Special Counsel's memorandum on workplace privacy. [3]

Therefore, pursuant to Rule X, (3)(g) and Rule XI of the Rules of the House of Representatives, we respectfully request that you provide the following information no later than August 8, 2012:

1. The legal analysis requested in our June 25, 2012 letter. This analysis was not included in your response received on July 18, 2012.

---

[1] [1] Federal Business Opportunities. Solicitations by TSA, June 20, 2012.

[2] Letter, Transportation Security Administration's Administrator John Pistole to Congressman Bennie G. Thompson July 18, 2012. Response to Congressman Thompson's letter to TSA re Spyware RFP.

[3] Memorandum on Workplace Privacy, Office of Special Counsel to Government Agencies. June 2012.

2. In your letter, you cite that TSA is committed to the guidance outlined by the United States Office of Special Counsel's (OSC) *Memorandum for Executive Departments and Agencies Regarding Agency Monitoring Policies and Confidential Whistleblowers Disclosure to the Office or Special Counsel and to Inspectors General.* The OSC memo asks agencies to review their policies, please provide copies of current policies on monitoring employees.

3. In your letter, you indicated that TSA's proposed use of this software would be in compliance with OSC guidance. Please provide a copy of documentation from the OSC which verifies this statement.

4. In your letter, you reference that this proposed technology would be used with a "specific user who has been identified as a potential threat" and a "predicate that suggests the user poses a threat." This language implies a criminal justice standard of reasonable suspicion but does not appear to have any specific legal meaning.

    a. Please provide us with the definition TSA will use to determine "specific user who has been identified as a potential threat" and "predicate that suggests the user poses a threat."

    b. If an employee is deemed to fit either definition, please provide a narrative explaining the process by which TSA would determine and substantiate the factual sufficiency of such allegations prior to use of this program.

5. Given that the universe of employees who present a potential threat is not likely to be large, please explain why the current method, which permits monitoring of these communications paths manually, would not be sufficient.

6. On a fiscal year basis, please provide the anticipated cost for the purchase and maintenance of "insider threat software."

If you have any questions or concerns regarding the matters discussed above, please contact Cherri Branson, Chief Counsel for Oversight, at 202-226-2616.

Sincerely,

Bennie G. Thompson
Ranking Member

Sheila Jackson Lee
Ranking Member
Subcommittee on Transportation Security