



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

October 3, 2012

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

Dear Administrator Pistole:

On July 25, 2012, we wrote 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."<sup>1</sup> Despite requesting that you respond to our inquiry by August 8, 2012, we have yet to receive your response.

Today, the Department of Homeland Security Office of Inspector General (OIG) released a report titled "*Transportation Security Administration Has Taken Steps To Address the Insider Threat But Challenges Remain.*"<sup>2</sup> The OIG report reveals that TSA does not have policies, procedures, and a risk management plan pertinent to the insider threat currently in place. Further, the report reveals that TSA has yet to implement an insider threat training and awareness program for the entire TSA workforce. To our dismay, TSA failed to concur with two common sense low cost OIG recommendations aimed at protecting against the loss of sensitive data from TSA's networks.

The findings of the OIG report and TSA's rationale for failing to concur with the OIG's low cost recommendations for protecting sensitive data raise serious questions regarding TSA's June 20, 2012 sources sought notification posted on the Federal Business Opportunities Website. Pursuant to Rule X cl. 3(g) and Rule XI of the United States House of Representatives, in addition to responses to our requests for information contained in our letter of July 25, 2012, please provide the following information not later than October 17, 2012.

1. A detailed description of TSA's current expenditures related to the information technology insider threat.

---

<sup>1</sup> Federal Business Opportunities. Solicitations by TSA, June 20, 2012.

<sup>2</sup> OIG-12-120

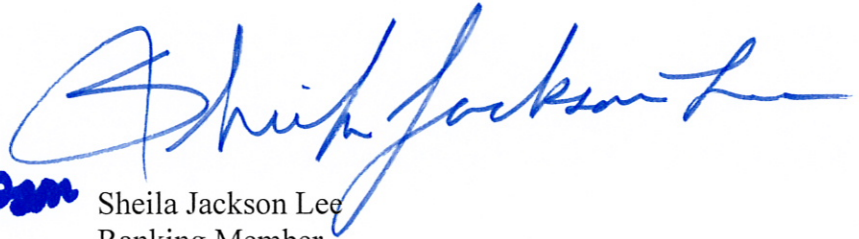
2. An estimate of the anticipated lifecycle cost of the "Insider Threat Software" TSA solicited on July 25, 2012 in a posting on the Federal Business Opportunities Website.
3. The date by which TSA will have policies, procedures, and a risk management plan pertinent to the insider threat in place accompanied by a detailed description of the policies, procedures, and risk management plan.
4. The date by which TSA will implement an insider threat training and awareness program for the entire TSA workforce along with a detailed description of the program.

Thank you for your attention to this matter. If you have any questions about this request, 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

Enclosure: Letter of July 25, 2012 regarding Insider Threat Software



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