



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

June 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 regarding a recent solicitation for an “enterprise insider threat software package.” The solicitation, posted by the Transportation Security Administration (TSA) on the Federal Business Opportunities website on June 20, 2012,<sup>1</sup> seeks to acquire technology that would “monitor and obtain visibility into users' actions.”

According to TSA’s solicitation, the monitoring and surveillance technology will allow TSA to observe working employees performing all TSA operations. Specifically, the solicitation calls for capability requirements, which include:

Ability to monitor user activities through:

- Keystroke monitoring/logging
- Chat monitoring/logging
- Email monitoring/logging
- Attachment monitoring/logging
- Website monitoring/logging
- Network activity monitoring/logging
- Files transferred monitoring/logging
- Document tracking monitoring/logging
- Screenshot capture
- Program activity monitoring/logging

---

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

[https://www.fbo.gov/?s=opportunity&mode=form&id=6b790f932382cb2aa5b5c7249820ac72&tab=core&\\_cview=0](https://www.fbo.gov/?s=opportunity&mode=form&id=6b790f932382cb2aa5b5c7249820ac72&tab=core&_cview=0). Accessed on June 22, 2012.

In addition to these monitoring requirements, the solicitation indicates that the technology should be able to assure that the “end user must have neither the ability to detect this technology” nor the ability to “kill the process or service.”

In an interesting timing of events, also on June 20, 2012, the United States Office of Special Counsel issued a memorandum to all executive departments and agencies reminding them of existing guidelines protecting the rights of the Federal workforce against unlawful monitoring of employee communications via the use of electronic surveillance.

As noted by the Office of Special Counsel, in certain situations the lawful monitoring of an employee may be warranted by the Federal government, however, thoughtful evaluation of the practices conducted by agencies must be constantly undertaken to ensure that such practices garner proper restrictions that afford them to operate in a legal manner. Additionally, OSC cautioned that the:

“deliberate targeting by an employing agency of an employee’s submission (or draft submissions) to the OSC or an IG, or deliberate monitoring of communications between the employee and the OSC or IG in response to such a submission by the employee, could lead to a determination that the agency has retaliated against the employee for making a protected disclosure. The same risk is presented by an employing agency’s deliberate targeting of an employee’s emails or computer files for monitoring simply because the employee made a protected disclosure.”<sup>2</sup>

To underscore its willingness to examine violations of monitoring policy, the Office of Special Counsel broadened the scope of its existing investigation into the surveillance of employees’ emails by the Food and Drug Administration (FDA). FDA acknowledged that it monitored emails at the Center for Devices and Radiological Health to congressional investigators and the OSC after the employees reported coercion to approve unsafe or harmful medical devices.<sup>3</sup>

While the law governing TSA employees does not afford specific protections to ensure employee whistleblower protections, the agency is not completely insulated from the affects of the Constitution. It would seem that installation of the type of technology sought in the solicitation would enable TSA to monitor employee communications with the OSC, the Department’s Office of Inspector General and the Congress of the United States. It is difficult to see how this serious infringement of Constitutionally protected rights would provide a concomitant increase in the nation’s security.

---

<sup>2</sup> *Memorandum for Executive Departments and Agencies Regarding Agency Monitoring Policies and Confidential Whistleblowers Disclosure to the Office of Special Counsel and to Inspectors General*, U.S. Office of Special Counsel, June 20, 2012.

<sup>3</sup> *Administration warns agencies about monitoring staff email*, Washington Post, June 22, 2012.

Clearly, the need to assure that employees are able to provide information to Congress or investigative entities within the Federal government has long been recognized. Thus, the nature of TSA's recently issued solicitation appears to contradict well-settled policies concerning the ability of Federal employees to communicate with investigative authorities without fear of retaliation.

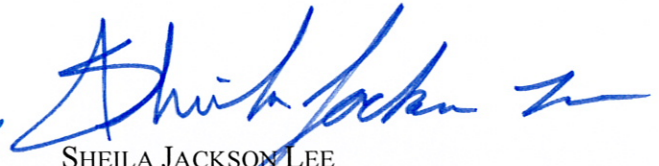
In sum, we strongly recommend that TSA immediately withdraw this solicitation and refrain from attempting to acquire technology with similar capabilities. Further, please provide the Committee with TSA's legal analysis concerning this solicitation and the aforementioned June 20<sup>th</sup> Memorandum from the Office of Special Counsel no later than July 9, 2012.

Thank you for your prompt attention in this matter. If you have any questions please contact Cherri Branson, Chief Counsel for Oversight, Committee on Homeland Security, Democratic Staff, at (202) 226-2616.

Sincerely,



BENNIE G. THOMPSON  
Ranking Member



SHEILA JACKSON LEE  
Ranking Member  
Subcommittee on Transportation  
Security