National Security

Intelligence security initiatives have chilling effect on federal whistleblowers, critics say

By Scott Higham July 23 at 10:51 AM

Follow @ScottHigham1

In early April, Sen. Charles E. Grassley (R-Iowa) summoned FBI officials to his Capitol Hill office. He said he wanted them to explain how a program designed to uncover internal security threats would at the same time protect whistleblowers who wanted to report wrongdoing within the bureau.

The meeting with two FBI officials, including the chief of the bureau's Insider Threat Program, ended almost as soon as it began. The officials said the FBI would protect whistleblowers by "registering" them. When Grassley's staffers asked them to elaborate, the FBI

officials declined to answer any more questions and headed for the door.

“We’re leaving,” said J. Christopher McDonough, an FBI agent assigned to the bureau’s congressional affairs office, according to Senate staffers who attended the meeting.

The episode infuriated Grassley, a leading advocate for whistleblowers in Congress and the ranking Republican on the Senate Judiciary Committee, which oversees the FBI. Any effort to register whistleblowers, Grassley said, would “clearly put a target on their backs.”

The Insider Threat Program and a continuous monitoring initiative under consideration in the intelligence community were begun by the Obama administration after the leaks of classified information by former NSA contractor Edward Snowden and Army Pvt. Chelsea Manning, and the Navy Yard shootings by Aaron Alexis, who used his security clearance to gain access to the base.

The programs are designed to prevent leaks of classified information by monitoring government computers and the behavior of employees.

Grassley said the episode with the FBI illustrates how federal agencies are setting up internal security programs without giving careful consideration to how those programs could dissuade whistleblowers from

coming forward. He decried the lack of transparency of many of the programs and said finding out how federal agencies intend to protect whistleblowers has not been easy.

“The Insider Threat Program has the potential for taking the legs out from underneath all of the whistleblower protections we have,” Grassley said in a recent interview.

The head of the FBI’s Insider Threat Program, Greg Klein, and the congressional affairs agent, McDonough, did not return calls for comment. An FBI spokesman said the bureau does not plan to register whistleblowers. He said there was a misunderstanding about the nature of the briefing with staffers for Grassley, Sen. Patrick J. Leahy (D-Vt.), the committee chairman, and a law enforcement official who is assigned to the Senate Judiciary Committee. The spokesman noted that the FBI has a whistleblower training program for employees and a whistleblower protection office.

“We continue to work with Senator Grassley’s office and address whatever concerns the senator has,” FBI spokesman Paul Bresson said. “We recognize the importance of protecting the rights of whistleblowers.”

Grassley is part of a growing chorus of lawmakers on Capitol Hill and attorneys for whistleblowers who warn that the little-publicized Insider Threat Program and another initiative under consideration for the

intelligence community threaten to undermine the ability of federal workers to report wrongdoing without retaliation.

Together, the programs cover millions of federal workers and contractors at every government agency.

In February, Director of National Intelligence James R. Clapper Jr. testified before the Senate Armed Services Committee that a system was being considered to continuously monitor the behavior of employees with security clearances “on the job as well as off the job.” Another senior national intelligence official, Brian Prioletti, testified before a House Homeland Security subcommittee in November that pilot programs had been set up to study monitoring “publicly available electronic information, to include “social media sites.”

A senior intelligence official said a continuous monitoring program is in the process of being set up and it will initially include federal employees who hold top-secret security clearances. The official said there are no plans to monitor employees after hours while they are using non-U.S. government computer systems.

The insider threat and monitoring programs have caught the attention of lawmakers and whistleblower lawyers.

“I think it’s time to put up the caution light here,” said Sen. Ron Wyden (D-Ore.), a member of the Senate Intelligence Committee who has been a leading advocate for whistleblowers.

While Wyden included a provision in the most recent Intelligence Authorization Act prohibiting retaliation against whistleblowers, he said he remains concerned about the impact the Insider Threat Program and the continuous monitoring initiative will have on the willingness of federal workers to come forward.

“This really has the potential for abuse, and I think it could have a chilling effect on the public’s right to know and effective oversight of our government,” Wyden said. “I want people to know that there is a difference between a whistleblower who is trying to do the right thing and people who are trying to gratuitously make trouble or want to leak classified information.”

The head of the Intelligence Community Whistleblowing & Source Protection program, created last year as part of the Intelligence Community Inspector General’s Office, said he is working to ensure that employees who want to report wrongdoing can do so anonymously and without reprisals.

“The critical thing is to maintain confidentiality,” Dan Meyer said. He said he is in the process of preparing training materials for intelligence officers and

spreading the word that employees can come to him anonymously through third parties. They do not need to use their computers or cellphones to contact him.

“A pen and a pad can be very useful,” Meyer said.

If an employee has verifiable information about wrongdoing, a presidential directive takes effect, providing employees with protection against retaliation, whether they are working at the CIA, the NSA or any other intelligence agency.

“We are in the process of making a systematic, cultural change and getting everyone on board,” Meyer said.

After Manning’s disclosures to WikiLeaks four years ago, President Obama signed Executive Order 13587, directing government agencies to assess how they handle classified information. On Nov. 28, 2010, the Office of the National Counterintelligence Executive issued a memo to senior government agency officials, advising them to identify insider threats within their offices and among their workforces.

The memo suggested using psychiatrists and sociologists to assess changes in behavior of employees.

“What metrics do you use to measure ‘trustworthiness’ without alienating employees?” the counterintelligence office asked the agency chiefs. “Do you use a psychiatrist or sociologist to measure: Relative

happiness as a means to gauge trustworthiness? Despondence and grumpiness as a means to gauge waning trustworthiness?"

"Most whistleblowers want to work within the system, but by creating this paranoid super-system of monitoring, they are going to go outside the system," said Lynne Bernabei, a partner at Bernabei & Wachtel in Washington who has been representing whistleblowers for nearly 30 years."It will only increase hostility between the government and really serious federal employees who are trying to improve the system. Turning the security apparatus against its own people is not going to work."

Whistleblower lawyers said they understand the need to protect classified information but believe some of the new programs go too far.

"There are legitimate reasons for employers to be on the lookout for people who might be leaking classified information, but this will obviously have a chilling effect on employees who might want to blow the whistle," said Jason Zuckerman, who served as the senior legal adviser to the U.S. Office of Special Counsel, the federal agency charged with protecting whistleblowers, and now represents whistleblowers across the country. "What they are saying to employees is if you suspect that one of your co-workers is a possible whistleblower, you should report them."

Michael German is a former undercover FBI agent who knows firsthand the difficulties associated with reporting wrongdoing within a government agency. He said the FBI retaliated against him after he alerted Congress to problems with counterintelligence efforts and he wound up leaving the bureau after a 16-year career.

He called the Insider Threat Program a “dangerous” initiative that will deter whistleblowers from coming forward.

“These agencies have long treated whistleblowers as security threats and this makes things even worse,” said German, now a senior national security fellow at the Brennan Center for Justice at New York University School of Law. “The failure to create effective pathways to bring information to Congress and ultimately to the public is what leads to these massive leaks.”

Mark S. Zaid specializes in representing whistleblowers in the intelligence community and the military. He said the administration is moving too quickly, with little or no oversight from Congress.

“Have there been any congressional hearings? Have there been any panels appointed to look into this?” Zaid asked. “No, but they are implementing these programs and the ramifications are going to be felt for years to come. They are using a very big net to catch a few small fish, and they are going to hurt a lot of good people in the process.”

Scott Higham is a member of the investigations unit of The Washington Post.