DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

JUL 25 2014

The Honorable Charles Grassley
United States Senate
Washington, DC 20510

The Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senators Grassley and Wyden:

Thank you for your June 18, 2014 letter articulating concerns regarding the potential application of continuous monitoring and continuous evaluation to the Legislative Branch and potential impact on whistleblower protections. I hope this letter will provide more insight into these processes and, in turn, will allay your concerns.

As an initial matter, it is useful here to define and distinguish the terms "continuous evaluation (CE)" and "user activity monitoring (UAM)." [1]

Continuous Evaluation

CE is a process currently under development that, when completed, is designed to enhance the personnel security process by ensuring that significant information relevant to an individual's continued suitability for access to classified information is identified more quickly than the current periodic reinvestigation process allows. Currently an individual with access to Top Secret information undergoes a periodic reinvestigation every five years – and as you are aware, due to resource constraints the period between periodic reinvestigations can in many instances be even longer. Under the current system, for example, somebody arrested for a violent crime could enjoy continued access to Top Secret information or classified facilities for five years or more before the crime is discovered during the individual's periodic reinvestigation. CE is designed to ensure that does not happen, by conducting automated and ongoing checks of several commercial and government databases to identify information that has potential adjudicative value for determining an individual's suitability for continued access to classified information and facilities.

User Activity Monitoring

UAM is defined as the technical capability to observe and record the actions and activities of an individual on a Government device, computer or information system, in order to detect insider threats and to support authorized investigations. It could include key stroke

[1] Another term, "continuous monitoring (CM)," refers to the continuous and ongoing monitoring necessary to maintain a current status for security systems (i.e., the health of the network). For example, CM on a critical information system could potentially identify efforts by a foreign intelligence service to hack into the system, or identify the introduction of malware into a sensitive information system. Because CM is not relevant to the questions raised in your letter, it is not further addressed here.

monitoring, as well as the collection of e-mails, chats, screen captures, and so forth. For example, if it was discovered that an individual with access to classified information was secretly meeting with someone from a hostile country, his activities on Government computers could be monitored to help determine whether he was stealing classified information and selling it to the hostile country – for example, by revealing what he is accessing, printing, or downloading.

Applicability of CE and UAM to the Legislative Branch

You first ask whether I believe that the Executive Branch has the authority to engage in CE of Members of Congress with access to classified information and of Legislative Branch employees with security clearances. With respect to Members of Congress, because CE applies to individuals who have been "determined eligible" for access to classified information through security clearance processes pursuant to EO 12968, and because Members of Congress do not undergo those security clearance processes or eligibility determinations, by definition CE would not apply to Members of Congress. Unlike Members, however, Legislative Branch employees undergo the security clearance process and are determined eligible for access to classified information by the Executive Branch. Nevertheless, in my previous testimony, I did not suggest that we plan to apply CE to Legislative Branch employees. To be clear, we have no such intention, and indeed the relevant Executive Orders regarding CE apply specifically to Executive Branch employees. Accordingly, we have focused implementation of CE on covered individuals employed by Executive Branch agencies in accordance with EO 13467 (which to be clear, however, would include employees of Executive Branch agencies on detail to the Legislative or Judicial Branch).

With respect to your second question about monitoring of Members of Congress and Legislative Branch employees, in general those individuals will not be subject to UAM because their classified networks are not included in the definition of national security systems (NSS) for which monitoring is required. National security systems must comply with the Committee on National Security Systems (CNSS) Directive No. 504, which requires national security systems to have the capability to collect user activity data, including key stroke monitoring, email, chats, screen captures, and file shadowing – and users are notified of this monitoring by a banner appearing at log-on. Directive 504 derives its definition of a national security system from the Federal Information Security Management Act, which in turn defines a national security system as, among other things, being used or operated by an agency, a contractor of an agency, or another organization on behalf of an agency (44 U.S.C. § 3542). An agency is defined to include Executive Branch entities and certain independent agencies, but does not include the Legislative Branch (44 U.S.C. § 3502). Because no internally owned or operated Legislative Branch network qualifies as a national security system, UAM by the Executive Branch is accordingly neither required nor conducted. To be clear, however, when Legislative Branch personnel access a national security system used or operated by the Executive Branch, they are of course subject to UAM on that particular system.

Impact of CE and UAM on Whistleblower Protections

I share your views on the importance of ensuring that whistleblowers are not targeted for extra scrutiny or otherwise feel they cannot report issues of concern. Any sort of retaliation

against legitimate whistleblowers is a violation of federal law, and we must vigorously enforce that law.

The proposed framework for CE is being vetted by ODNI legal and privacy officials to ensure compliance with applicable laws, civil liberties and privacy policies. CE's collection and evaluation methodology is limited to government, commercially available, and public records containing information about an individual's behavior that is of specific adjudicative concern, such as financial and criminal activity and foreign travel. Such security and counterintelligence-relevant information has always been an essential element of security clearance eligibility determinations, and CE will simply facilitate the collection and discovery of this information on an ongoing basis to fill gaps in time between periodic reinvestigations. I am not aware of any impact CE could potentially have on whistleblowers.

With respect to UAM, there is a need to clearly distinguish whistleblowers from individuals who make unauthorized disclosures by taking it upon themselves to decide what classified information should be disclosed to the public. Whistleblowers make use of formal reporting procedures that will provide protection to the classified information and to the whistleblower. Any disclosure of classified information falling outside of these established procedures constitutes an unauthorized disclosure - not protected whistleblowing - and falls into the realm of insider threat behavior.

In the event a protected disclosure by a whistleblower somehow comes to the attention of personnel responsible for monitoring user activity, there is no intention for such disclosures to be reported to agency leadership under an insider threat program. Protected disclosures, as defined in PPD 19, would not manifest in the kinds of anomalous behaviors and activities that UAM is designed to detect, and therefore would generally not come to the attention of personnel responsible for monitoring user activity. Some agencies currently conducting UAM are also training their investigators to screen out protected communications, and such training can be made universal. Further, guidance provided by the National Insider Threat Task Force to agencies implementing their Insider Threat Programs emphasizes the need for close collaboration with agency counsel, as well as privacy and civil liberties officials, to ensure that the legal protections afforded personnel, including whistleblower protections, are proactively considered and addressed in implementation. Moreover, the Inspector General of the Intelligence Community, in coordination with the Intelligence Community Inspectors General Forum, is currently examining the potential for internal controls that would ensure whistleblower-related communications remain confidential, while also ensuring the necessary UAM occurs.

The Intelligence Community is firmly committed to the tenets of PPD 19 ensuring that employees of the IC or other individuals that have access to classified information can -- confidentially, and without fear of reprisal -- report fraud, waste and abuse in a manner that protects classified information. Intelligence Community Directive 120, *Whistleblower Protection*, that I signed in March of this year establishes community-wide policy to this effect and directs Intelligence Community elements to establish policies and processes consistent with PPD 19.

I share your belief that the scope and implementation of the CE and components of the Insider Threat Program are critical issues requiring careful consideration. I sincerely hope the information in this letter will convey our continued commitment to ensuring that the implementation of these programs are consistent with law and with respect for the Constitutional principle of separation of powers. If you have additional questions, please contact Deirdre M. Walsh, Director of Legislative Affairs, at (703) 275-2474.

Sincerely,

James R. Clapper

cc: John O. Brennan
Director, Central Intelligence Agency