

# United States Senate

WASHINGTON, DC 20510

June 18, 2014

## VIA ELECTRONIC TRANSMISSION

Lt. Gen. James R. Clapper  
Director of National Intelligence  
Office of the Director of National Intelligence  
Washington, D.C. 20511

Dear Director Clapper:

Recent events, including testimony you provided before the Senate Committee on Armed Services, have raised concerns for us about plans to implement a policy of continuous monitoring of security clearance holders. We recognize the need to ensure that government employees are not unlawfully disclosing classified information, and that some heightened monitoring of certain clearance holders may be appropriate. However, there are constitutional, statutory, and prudential limits to that monitoring. We write to clarify the scope of this monitoring as applied to the Legislative Branch. We also write to urge that as the Office of the Director of National Intelligence (ODNI) develops and implements the monitoring of Executive Branch employees, it takes into account the need to ensure the ability of whistleblowers to report waste, fraud, and abuse, including anonymously if they so choose.

## Continuous Evaluation

On February 11, 2014, you testified before the Senate Committee on Armed Services:

We are going to proliferate deployment of auditing and monitoring capabilities to enhance our insider threat detection. We're going to need to change our security clearance process to a system of continuous evaluation. . . . What we need is . . . a system of continuous evaluation, where . . . we have a way of *monitoring their behavior, both their electronic behavior on the job as well as off the job*, to see if there is a potential clearance issue. . . .<sup>1</sup>

Recent versions of the Intelligence Authorization Act for Fiscal Year (FY) 2014 would amend 50 U.S.C. 3024(j) by adding a section that would require the Director of National Intelligence to:

(5) *ensure that the background* of each employee or officer of an element of the intelligence community, each contractor to an element of the intelligence community, and each individual employee of such a contractor

---

<sup>1</sup> *Current and Future Worldwide Threats to the National Security of the United States, Hearing Before the S. Committee on Armed Services, 113th Cong. (Feb. 11, 2014) (Testimony of James R. Clapper, Director of National Intelligence, Office of the Director of National Intelligence).*

who has been determined to be eligible for access to classified information *is monitored on a continual basis* under standards developed by the Director, including with respect to the frequency of evaluation, during the period of eligibility of such employee or officer . . . to determine whether such employee or officer . . . continues to meet the requirements for eligibility for access to classified information . . .<sup>2</sup>

### **Evaluation or Monitoring of Legislative Branch Employees**

Especially in light of recent events, we first ask that you confirm that you did not intend to suggest that Members of Congress or staff members in the Legislative Branch would be subject to continuous evaluation. The above legislation, which applies only to the Executive Branch, certainly does not support such a view. However, it appears from your remarks before the Armed Services Committee that you believed ODNI already had authority at the time to carry out such monitoring, at least of Executive Branch employees.

While the Executive Branch is responsible for conducting background checks for congressional staff in the normal course of approving their security clearances, any continuous evaluation or monitoring of holders of clearances in the Legislative Branch by the Executive Branch would raise serious issues related to the separation of powers and potentially violate fundamental privileges of the Legislative Branch guaranteed in the Constitution. Accordingly, so that we may discuss the serious constitutional issues implicated by any such claim, please provide an explanation as to whether you believe that the Executive Branch has the authority to engage in ongoing monitoring of Legislative Branch employees with clearances or Members of Congress with access to classified information.

### **The Need to Preserve Whistleblower Protections Under a System of Continuous Evaluation**

Even when such monitoring is limited to Executive Branch employees, any continuous evaluation must be subject to certain limitations and safeguards to preserve the rights and confidentiality of whistleblowers.

These rights are well established. In 1912, Congress passed the Lloyd-La Follette Act, which stated: "The right of employees, individually or collectively, to petition Congress or a Member of Congress, or to furnish information to either House of Congress, or to a committee or Member thereof, may not be interfered with or denied."<sup>3</sup>

Since 1998, a government-wide rider has appeared in every appropriations bill stating:

No part of any appropriation contained in this or any other Act shall be available for the payment of the salary of any officer or employee of the

---

<sup>2</sup> Title V, Sec. 501.

<sup>3</sup> 5 U.S.C. 7211.



Federal Government, who . . . prohibits or prevents, or attempts or threatens to prohibit or prevent, any other officer or employee of the Federal Government from having any direct oral or written communication or contact with any Member, committee, or subcommittee of the Congress in connection with any matter pertaining to the employment of such other officer or employee or pertaining to the department or agency of such other officer or employee in any way, irrespective of whether such communication or contact is at the initiative of such other officer or employee or in response to the request or inquiry of such Member, committee, or subcommittee.<sup>4</sup>

That same year, Congress passed the Intelligence Community Whistleblower Protection Act of 1998. Under its provisions, an intelligence community employee has the right to contact both the Inspector General<sup>5</sup> as well as the intelligence committees<sup>6</sup> with urgent concerns. According to the Intelligence Community Whistleblower Protection Act, such urgent concerns would include any action, such as any of the personnel practices prohibited by the Whistleblower Protection Act of 1989,<sup>7</sup> “constituting reprisal or threat of reprisal . . . in response to an employee’s reporting an urgent concern . . . .”<sup>8</sup> Such retaliation is explicitly prohibited:

Any employee who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or threaten to take any action against any employee as a reprisal for making a complaint or disclosing information to an Inspector General . . . .<sup>9</sup>

On October 10, 2012, Presidential Policy Directive 19 (PPD 19) reiterated this prohibition and extended it to any action affecting an employee’s eligibility for access to classified information. PPD 19 directed the head of each intelligence community element to certify to you that “the personnel policies that apply to that element provide a process for employees to seek review of Personnel Actions they allege to be in violation of this directive . . . .”<sup>10</sup> In the case of a violation, the agency Inspector General “may recommend that the agency take specific corrective action to return the employee . . . to the position such employee would have held had the reprisal not occurred.”<sup>11</sup> The FY 2014 Intelligence Authorization Act which passed the Senate on June 11, 2014 would make these protections statutory.

---

<sup>4</sup> Sec. 713, Consolidated Appropriations Act of 2012, Pub. L. No. 112-74, 125 Stat. 931, 932, as continued by Section 103, Pub. L. 112-175 (2012) and Sec. 1102, Pub. L. 113-6 (2013).

<sup>5</sup> 5 U.S.C. App. § 8H(a)(1); see also, for example, 50 U.S.C. § 3517(d)(5), which establishes parallel procedures for the Inspector General of the Central Intelligence Agency.

<sup>6</sup> 5 U.S.C. App. § 8H(d).

<sup>7</sup> 5 U.S.C. § 2302.

<sup>8</sup> 5 U.S.C. App. § 8H(h)(1)(C).

<sup>9</sup> 5 U.S.C. App. § 7(c).

<sup>10</sup> PPD 19, A

<sup>11</sup> PPD 19, *Id.*

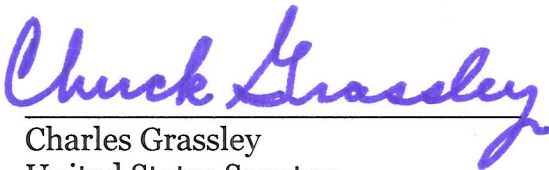
Despite these measures, whistleblower protection provisions are never perfect. Sometimes confidentiality is the best protection a whistleblower has. Thus, not only are federal employees protected in making disclosures to Inspector Generals, the Inspector General Act of 1978 directs that “[t]he Inspector General shall not, after receipt of a complaint or information from an employee, disclose the identity of the employee without the consent of the employee, unless the Inspector General determines such disclosure is unavoidable during the course of the investigation.”<sup>12</sup>

If whistleblower communications with Inspectors General or with Congress are routinely monitored and conveyed to agency leadership, it would defeat the ability to make protected disclosures confidentially, which is especially important in an intelligence community context. Truly meaningful whistleblower protections need to include the option of a legitimate channel for confidential disclosures. Inspectors General and Congress provide such an option. However, if potential whistleblowers believe that disclosing waste, fraud or abuse means putting a target on their backs for retaliation, they will be intimidated into silence. The failure to provide such protected alternatives could result in whistleblowers choosing to make unprotected disclosures in public forums, with potential negative consequences for national security.

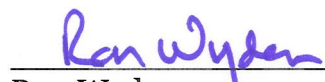
In particular, any monitoring of employees’ *“electronic behavior on the job as well as off the job”* needs to include safeguards to prevent the chilling of legitimate whistleblower communications and protect the confidentiality of any legally privileged information. Procedural safeguards to prevent the targeting of whistleblowers for extra scrutiny as well as minimization requirements to avoid collecting protected communications are some examples of the sorts of safeguards that should be developed. If captured inadvertently, protected disclosures certainly should never be routed back to an official involved in any alleged wrongdoing reported by the whistleblower.

We believe it is critical that these issues be carefully considered and resolved before fully implementing any policy of continuous monitoring. Therefore, please explain by July 15 how you intend to address these issues.

Sincerely,



Charles Grassley  
United States Senator

  
\_\_\_\_\_  
Ron Wyden  
United States Senator

cc: The Honorable John O. Brennan, Director  
Central Intelligence Agency

---

<sup>12</sup> 5 U.S.C. App. § 7(b).