SOCIAL SECURITY

The Commissioner

July 08, 2013

James R. Clapper
Director of National Intelligence

Dear Mr. Clapper:

In accordance with your December 12, 2012 and April 11, 2013 memorandums, I certify that the Social Security Administration has a process for reviewing alleged whistleblower reprisal actions, as outlined in Section B of Presidential Policy Directive 19 (PPD-19), *Protecting Whistleblowers with Access to Classified Information,* issued on October 10, 2012. Our policy ensures employees eligible for access to classified information can report fraud, waste, and abuse. It also prohibits retaliation against employees for such reporting. Our review process:

- Permits employees to appeal actions affecting their eligibility for access to classified information they allege to be in violation of PPD-19;
- Is consistent with policies and procedures used to adjudicate security clearances under EO 12968, *Access to Classified Information*, as amended, and protects classified information and intelligence sources and methods;
- Provides protections for classified national security information and intelligence sources and methods;
- Includes our Inspector General (IG) review to determine whether an action affecting eligibility violates PPD-19;
- Ensures I have an opportunity to consider IG recommendations if any; and
- Ensures that employees are aware of the availability of an external review (i.e., an External Panel Review chaired by the IG of the Intelligence Community).

I am enclosing our *Security Clearance Administrative Review Process Policy.* Your staff may contact Jonas Garland, our Associate Commissioner for the Office of Security and Emergency Preparedness, at 410-965-6660, or at jonas.garland@ssa.gov for questions related to this policy.

Sincerely,

Carolyn W. Colvin

Carolyn W. Colvin
Acting Commissioner

Enclosure

Social Security Administration

Security Clearance Administrative Review Process Policy

July 2013

I. INTRODUCTION

Classified information is information the United States Government considers sensitive and requires secrecy based on national security needs. The Government restricts access to classified information to individuals with a formal security clearance at the appropriate level and with a need to know the information. The Government grants a security clearance to an individual allowing him or her access to certain classified information after the completion of a thorough background check.

To ensure we properly safeguard classified information we handle and store at our controlled facilities, we maintain a security clearance process to determine our employees' eligibility to access classified information. Our oversight protocols ensure our handling and protection of classified materials complies with all applicable orders, laws, and regulations.

II. AUTHORITY

Our Security Clearance Administrative Review Process Policy complies with the following laws, directives, and Executive Orders (EO):

- Presidential Policy Directive (PPD) 19, *Protecting Whistleblowers with Access to Classified Information*; October 10, 2012
- EO 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*; October 7, 2011
- 32 Code of Federal Regulations (CFR) Parts 2001 [*Classified National Security Information Final Rule*, June 28, 2010] and 2003 [*Interagency Security Classification Appeals Panel Bylaws, Rules, and Appeal Procedures, July 9, 2012]*
- EO 13526, *Classified National Security Information Memorandum*; December 29, 2009
- EO 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*; July 2, 2008
- EO 12968, *Access to Classified Information*; August 2, 1995
- 5 United States Code § 2302(b)(8), Whistleblower Protection, December 2005
- 5 CFR Part 1201, Merit System Protection Board, Procedures for Appellate Cases

III. DEFINITIONS

As they apply to civilian employees, terms used in this policy have the following definitions:

- **Employee of the Social Security Administration (SSA)** - Any civilian who is an assignee, detailee, or employee with SSA.

- **Personnel Action** - Any action that affects or has the potential to affect the employment opportunities of a job applicant or the current position or career of an SSA employee. Such actions include any appointment; promotion; disciplinary or corrective action; detail, transfer, or reassignment; reinstatement, restoration, or reemployment; decision concerning pay, benefits, awards, education, or training; and any other significant change in duties or responsibilities that is inconsistent with the employee's salary or grade level.

- **Protected Disclosure** –

  (1) A lawful disclosure of unclassified information by an employee or applicant for employment, which the employee or applicant reasonably believes evidences:

  - violation of any law, rule, or regulation; or

  - mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety; and

  - such disclosure is not specifically prohibited by law and if the information is not specifically required by or pursuant to executive order to be kept secret in the interest of national defense or the conduct of foreign affairs.

  (2) A lawful disclosure of classified information by an employee or applicant for employment to any Member of Congress or to any other civilian employee duly designated by law to receive disclosures of information, including a disclosure of information that is otherwise specifically prohibited by law, or information that is otherwise specifically required by or pursuant to executive order to be kept secret in the interest of national defense or the conduct of foreign affairs which the employee or applicant reasonably believes evidences:

  - violation of any law, rule, or regulation; or

  - mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

- **Reprisal** - Taking or threatening to take an unfavorable personnel action, or withholding or threatening to withhold a favorable personnel action concerning an employee of SSA or an applicant for employment for making, preparing to make, or for supporting one who makes or is preparing to make a protected disclosure.

- **Whistleblower** - An employee or job applicant who makes a protected disclosure by exposing alleged misconduct or dishonest or illegal activity occurring in an organization.

IV. POLICY

Our policy for protecting classified information and providing whistleblower protections comply with PPD-19. PPD-19 requires agencies to ensure that employees who are

eligible for access to classified information can effectively report waste, fraud, and abuse while protecting classified national security information. Our employees with security clearances have two mechanisms for reporting waste, fraud, and abuse related to our programs and operations, while protecting classified information. First, employees can report PPD-19 related matters to the Office of Inspector General (OIG) Whistleblower Ombudsman using the email address whistleblower.ombudsman@ssa.gov or call the Whistleblower Ombudsman Hotline at (855) 439-4606 or extension 3-1800 for Headquarters employees. In addition, our employees can report fraud, waste, and abuse using the OIG's fraud hotline (1-800-269-0271) or via an Internet form (http://eis.ba.ssa.gov/oig/hotline/index.htm).

Our policy also includes a process for employees to appeal actions negatively affecting their eligibilities for access to classified information. The review process complies with EO 12968, Section 5.2, *Review Process for Eligibility to Classified Information.*

In accordance with PPD-19, our policy ensures an employee is free from reprisal for making, preparing to make, or for supporting someone who makes a protected disclosure. The OIG for SSA will investigate any allegation of reprisal against an employee who makes or prepares to make a protected disclosure. We will take appropriate corrective and disciplinary action for any personnel action taken, withheld, or threatened in reprisal against an employee for making or preparing to make a protected disclosure or for supporting one who makes such disclosure.

This policy does not authorize any individual to violate the terms of a current and valid SSA nondisclosure agreement.

- Responsibilities

  - The Commissioner of Social Security – has overall responsibility for our agency's Security Clearance Administrative Review Process Policy.

  - The Deputy Commissioner for Budget, Finance and Management – has executive managerial oversight of the policy's implementation.

  - The Associate Commissioner for the Office of Security and Emergency Preparedness – is responsible for agency intelligence-related matters and performs the following delegated functions:

    - Federal Senior Intelligence Coordinator – works on matters pertaining to intelligence and collaborates with the Office of the Director of National Intelligence;

    - Insider Threat Program Senior Official – enforces the agency's Insider Threat Program to mitigate risks of insider threats and elevates critical issues involving classified information to the appropriate officials; and

- Information Sharing and Safeguarding Senior Official (ISSSO) – ensures the overall integrity of our information sharing and safeguarding program in compliance with EO 13587.

The ISSSO reviews employee requests for security clearances and approves or denies such requests based on employees' need to know classified information. In addition, the ISSSO conducts an annual assessment of employees' job duties to determine whether employees with access to classified information should retain their security clearances.

The Office of Human Resources' Center for Personnel Security and Project Management (CPSPM) facilitates the background investigation process for security clearances.

- Security Clearance Levels

The agency provides security clearances for three levels of classified information:

- Top Secret – applies to information where the unauthorized disclosure could cause exceptionally grave damage to the national security;
- Secret – applies to information where the unauthorized disclosure could cause serious damage to the national security; and
- Confidential – applies to information where the unauthorized disclosure could cause damage to the national security.

- Security Clearance Decisions

- Approvals

If the ISSSO determines that an employee requires access to classified information to perform his or her job duties, the ISSSO forwards the request to CPSPM for processing. If the employee needs to access classified information for his or her job and passes the proper background investigation, CPSPM will approve the employee's request for a security clearance. The agency does not perform security clearance activities for contractors.

- Denials

CPSPM may deny an employee's request for a security clearance based on the results of the background investigation. When CPSPM denies or revokes a security clearance, it issues a letter to the employee advising him or her of the rights under the provisions of E.O. 12968.

Under EO 12968, an employee has the right to request a review of their denial and receive a written explanation of the basis for the determination; initiate a Freedom of Information Act/Privacy Act request for any documents, records, and reports upon which the revocation is based; reply in writing and be represented by counsel, at the employee's own expense; and appear personally to present relevant information before the deciding official in CPSPM. The letter will also advise the employee of the applicable rights and requirements under PPD-19.

Revocations

CPSPM can revoke a security clearance if it discovers disqualifying information about an employee's background, the employee fails to meet personal conduct requirements, or the employee breaches security clearance policies (e.g., leaks classified information). Should CPSPM revoke an employee's security clearance, CPSPM will advise the employee of his or her rights to request a review of the determination.

- Revocations Related to Whistleblower Activities

  If CPSPM revokes an employee's clearance, it will review its internal system of records to ensure the revocation was not due to the employee's involvement in whistleblower actions. CPSPM will not revoke an employee's security clearance due solely to his or her involvement in whistleblower activities.

- Appeals Process Related to Security Clearance Revocation

  The OIG will investigate allegations of reprisal against employees related to protected disclosure activity. If an employee believes our agency revoked his or her clearance based on a protected disclosure under the provisions of PPD-19, the employee has the right to appeal the revocation to the OIG at whistleblower.ombudsman@ssa.gov. The employee has 30 calendar days to appeal the revocation determination. We will not reinstate a security clearance during the appeals process. OIG will determine if a revocation violated PPD-19.

  In determining any appropriate corrective actions, the Commissioner will consider the OIG's findings and recommendations, based on the OIG's review to determine if an agency action affecting eligibility violated PPD-19. If the OIG and the Commissioner sustain the revocation decision, we will advise the employee of his or her right to appeal the determination to the Inspector General of the Intelligence Community.

- Rescissions

  The need for access to classified information correlates with the duties of an employee's job. When the ISSSO determines that an employee no longer needs access to classified information (e.g., if an employee changes jobs to one where a security clearance is not necessary), the ISSSO notifies CPSPM, and CPSPM will rescind the employee's security clearance.

- Annual Reassessment

We require an annual reassessment of all employees with a security clearance. The yearly assessment focuses on employees' continued need (or lack thereof) for access to classified information to perform their current assigned duties. The ISSSO sends an

annual questionnaire to employees with security clearances inquiring about their job duties. The ISSSO analyzes the information provided and determines if there is a continued need for an employee to hold a security clearance. If the need for a security clearance no longer exists, the ISSSO rescinds an employee's security clearance.

- Annual Training

  The ISSSO ensures that each employee with a security clearance receives training annually to maintain his or her security clearance. The training includes the proper safeguarding of classified information; risk to national security of a disclosure of classified information; security procedures; and the imposition of criminal, civil, or administrative sanctions if an individual fails to protect classified information from unauthorized disclosure. Beginning in 2013, the training will also cover the provisions of PPD-19.