

MEMORANDUM OF AGREEMENT BETWEEN FACILITIES, SECURITY AND CONTRACTING, THE PERSONNEL SECURITY APPEALS BOARD, AND THE OFFICE OF THE INSPECTOR GENERAL, U.S. OFFICE OF PERSONNEL MANAGEMENT ON ROLES AND RESPONSIBILITIES FOR IMPLEMENTING PRESIDENTIAL POLICY DIRECTIVE 19

Background and Purpose.

This Memorandum of Agreement implements Presidential Policy Directive 19 (PPD-19) of October 10, 2012, *Protecting Whistleblowers with Access to Classified Information*, at the U.S. Office of Personnel Management (OPM).

Part B of PPD-19 provides that "Any officer or employee of an executive branch agency who has authority to take, direct others to take, recommend, or approve any action affecting an employee's Eligibility for Access to Classified Information shall not, with respect to such authority, take or fail to take, or threaten to take or fail to take, any action affecting an employee's Eligibility for Access to Classified Information as a reprisal for a Protected Disclosure." Part B further provides that each agency in possession of classified information must establish a "a review process that permits employees to appeal actions affecting Eligibility for Access to Classified Information they allege to be in violation of this directive." To the extent possible this review process must be "consistent with and integrated into the policies and procedures used to review security clearance determinations under Section 5.2 of Executive Order 12968 of August 2, 1995, as amended."

Further, as part of this review process, "the agency Inspector General shall conduct a review to determine whether an action affecting Eligibility for Access to Classified Information violated this directive and may recommend that the agency reconsider the employee's Eligibility for Access to Classified Information . . . and recommend that the agency take other corrective action to return the employee, as nearly as practicable and reasonable, to the position such employee would have held had the reprisal not occurred. An agency head shall carefully consider the findings of and actions recommended by the agency Inspector General." Once the Director has considered the Inspector General's findings and recommendations and rendered a final decision on whether to reconsider the employee's status, an employee may request additional review by an External Review Panel convened by the Inspector General for the Intelligence Community in accordance with PPD-19, which may also make a recommendation to the Director of OPM.

This Memorandum of Agreement prescribes the division of responsibilities between OPM's Office of the Inspector General (OIG), which has the responsibility to review whistleblower reprisal claims related to security clearance determinations under part B of PPD-19; and OPM's Facilities, Security and Contracting (FSC) and Personnel Security Appeals Board (PSAB), which share the responsibility, as delegated by the Director, to make and review security clearance determinations under E.O. 12968.

The Director has not delegated the function, under PPD-19, of determining whether to order

a corrective personnel action based on OIG's findings and recommendations. Although FSC and PSAB may grant or restore the security clearance of an employee who was subjected to a whistleblower reprisal, only the Director may order a corrective personnel action, and nothing in this Memorandum shall be interpreted as limiting or affecting the Director's role in these circumstances.

The Director also has not delegated the function, under PPD-19, of determining whether to grant or restore an employee's security clearance or to order corrective action based on the recommendations of an External Review Panel established under Part C of PPD-19. Nothing in this Memorandum shall be interpreted as limiting or affecting the Director's role in these circumstances.

### Definitions.

The following definitions apply to this memorandum.

*Corrective Action or Corrective Personnel Action* means reinstatement, reassignment, reasonable attorney's fees, other reasonable costs, back pay and related benefits, travel expenses, and compensatory damages, or any other corrective action authorized by law; but does not refer to the grant or restoration of a security clearance.

*Employee* means an employee of OPM as defined in 5 U.S.C. 2105.

*E. O. 12968* means Executive order 12968 of August 2, 1995, as amended.

*Security clearance* means access to classified information or eligibility for such access.

### FSC's Responsibilities.

1. When FSC issues an initial determination and written explanation to an employee, under section 5.2(a)(1) of E.O. 12968, that he or she does not meet the standards for access to classified information, FSC will enclose a copy of PPD-19 and will include, in its explanation, the following standard notice:

If you believe that you made a "protected disclosure" as defined in Presidential Policy Directive (PPD) 19 of October 10, 2012 [Enclosure (#)], and you believe that your access to classified information and/or eligibility for such access is being denied/revoked in reprisal for your protected disclosure, you must identify the circumstances of why you feel this applies in your written response and/or personal appearance. OPM will not consider, in its security clearance denial/revocation proceedings, any claim of reprisal that you raise after the response/personal appearance unless you can show that your claim *is* based on new and previously unavailable information.

If you do make a claim of reprisal in your response and/or personal appearance, your submission(s) will also be forwarded to OPM's Office of the Inspector General (OIG) for independent review and a recommendation of whether to take corrective action. You also have the right to submit your claim of reprisal directly to the OIG; however, OIG will not accept jurisdiction over complaints filed after the response/personal appearance stage,

unless you can show that your claim is based on new and previously unavailable information\_ Please note that, unlike many types of reports to the OIG, you cannot submit your claim of whistleblower reprisal anonymously, as OIG must inform FSC of any investigation so that FSC may consider OIG's findings and recommendations with regard to your case.

Whether you include your claim of reprisal in your response and/or personal appearance, or contact the OIG directly, the OIG will begin a review upon acceptance of your complaint. This review will be conducted without regard to the timing of the FSC's final decision regarding your security clearance and may be concluded before or after a decision is reached. However, the OIG, within its discretion, may request, and FSC, within its discretion, may grant, a stay of proceedings to allow time for OIG to conduct its review. The OIG review may include interviews and record reviews, and for this purpose the OIG may ask you to sign authorizations for releases of information; you may decline to sign such releases, but doing so may impede the full consideration of your complaint. After the OIG completes its review, OPM will consider the findings and any recommendations reported by the OIG and, if appropriate, may revise its decision regarding your Eligibility for Access to Classified Information.

Once you have exhausted the agency's administrative review process, you have the right to submit a request to the Inspector General of the Intelligence Community for an External Review Panel to consider your complaint of reprisal and recommend corrective action, if appropriate, to the agency.

2. If an employee's written response under section 5.2(a)(4) of E.O. 12968 includes a claim of reprisal, FSC will forward it to OIG, and will forward to OIG all subsequent correspondence with the employee concerning the security clearance proceeding.
3. If the employee requests a personal appearance under section 5.2(a)(7) of E.O. 12968, and raises a claim of reprisal in the personal appearance, FSC will promptly notify OIG of the claim. FSC will also promptly provide OIG any written submissions made by an employee during the personal appearance, and will forward to OIG all subsequent correspondence with the employee concerning the security clearance proceeding.
4. If FSC receives a complaint directly from an employee that the employee has been threatened with action affecting eligibility for a security clearance as reprisal for making a protected disclosure, FSC will promptly notify OIG of the claim, even if no such action has been initiated.
5. If FSC believes the claim of reprisal is unwarranted or has been resolved prior to OIG submission of its findings and recommendations, FSC may so notify OIG, without prejudice to OIG's right and responsibility to independently review the claim and to submit findings and recommendations.
6. FSC will normally agree to a request by OIG to suspend issuance of a final decision on a security clearance, when OIG needs additional time to conduct its review of a reprisal claim and to issue findings and recommendations related to the claim; but FSC will not ordinarily stay its decision for more than four weeks.

7. If OIG issues its findings and recommendations related to an employee's claim of reprisal before FSC issues a final decision on the employee's security clearance, FSC will fully consider OIG's findings and recommendations in reaching its final decision.

8. If FSC's final decision is to deny or revoke an employee's security clearance, and the employee appeals to the PSAB under section 5.2(a)(6) of E.O. 12968, FSC will forward to PSAB any OIG report of findings and recommendations, even if FSC receives it after making its final decision. FSC will also forward to PSAB all other material relied upon.

9. Alternatively if, after fully considering OIG's findings and recommendations, FSC's final decision is to grant or reinstate the employee's security clearance, FSC will promptly do so and will promptly alert the Office of the Director of the OIG's recommendations for corrective action, if any.

10. Following the exhaustion of all administrative redress within OPM as prescribed by part B of PPD-19, FSC will issue to the employee a notice of the right to an external review by the External Review Panel, enclosing a copy of the Intelligence Community Inspector General (IC IG) *External Review Panel Procedures Pursuant to Presidential Policy Directive - 19*, dated July 3, 2013.

11. As provided in part C of PPD-19, FSC will cooperate with OIG, the IC IG, and the External Review Panel and provide such information and assistance to such entities as they may request, as permitted by law.

#### PSAB's Responsibilities.

12. If an employee appeals the denial or revocation of a security clearance, and the employee raised a claim of whistleblower reprisal as described in this memorandum, PSAB will carefully review the OIG's findings and recommendations, if any, as well as all other material that FSC relied upon.

13. If, after fully considering any OIG findings and recommendations, PSAB's final decision is to grant or reinstate the employee's security clearance, PSAB will promptly order such action and will promptly alert the Office of the Director of OIG's recommendations for corrective action, if any.

14. If OIG does not issue its findings and recommendations until after PSAB has issued an appellate decision to deny or revoke the employee's security clearance, PSAB will reopen and reconsider its appellate decision giving full consideration to OIG's findings and recommendations.

15. As provided in part C of PPD-19, PSAB will cooperate with OIG, the IC IG, and the External Review Panel and provide such information and assistance to such entities as they may request, as permitted by law.

#### OIG's Responsibilities.

16. Upon receipt and acceptance of a complaint of reprisal or threatened reprisal prohibited

under PPD-19, whether directly from an employee or as described elsewhere in this memorandum, OIG will conduct a review of the employee's claim and will present its findings and recommendations to the Director, with copies to other agency officials including but not limited to the Associate Director, Facilities, Security and Contracting.

- a. Subject to the requirements of PPD-19, if the complaint is related to denial or revocation of a security clearance, OIG's findings and recommendations will address whether the denial or revocation of the employee's security clearance violated PPD-19; whether OPM should reconsider the employee's security clearance; and whether OPM should take other corrective action.
- b. Subject to the requirements of PPD-19, if the complaint is related to an alleged threat, OIG's findings and recommendations will address whether the alleged threat occurred and violated PPD-19, and whether OPM should take corrective action.
- c. Additionally, OIG may recommend appropriate disciplinary action and make other recommendations to the Director pursuant to its authority and powers under the Inspector General Act, as amended.

17. OIG will make every reasonable effort to complete its review and issue its findings and recommendations in a timely manner. OIG may request FSC to suspend issuance of a final decision on a security clearance, when necessary to give OIG adequate time to conduct its review and to issue its findings and recommendations.

18. Pursuant to the exercise of its authority and powers under the Inspector General Act, as amended, and its responsibilities under PPD-19, OIG review may include interviews and record reviews, and for this purpose OIG may ask the employee who submitted the complaint and other persons to sign authorizations for releases of information.

19. If an employee complains directly to OIG that his or her access to classified information and/or eligibility for such access is being or has been denied/revoked in reprisal for a protected disclosure, or that the employee has been threatened with such action, OIG will immediately advise FSC of the complaint and initiate a review pursuant to its responsibility under PPD-19.

20. With regard to complaints of reprisal in the form of denial/revocation of a security clearance, OIG will only accept jurisdiction over review of those complaints made prior to or during the written response/personal appearance before FSC, unless the employee shows that the complaint is based on new and previously unavailable information.

#### Effective Date.

This memorandum is effective from the date when it has been signed by all parties until it is superseded by agreement of the parties.

Limitations.

This memorandum creates no legal rights and obligations and must be implemented in accordance with applicable laws, rules, regulations, and presidential executive orders and directives. It may be supplemented by other agreements, policies and procedures.

Modification.

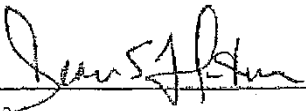
At any time, a Party may propose modification of this agreement. Proposed modifications shall only become effective upon unanimous agreement in writing by all Parties.

References (attached):

- A. Presidential Policy Directive 19 (PPD-19), *Protecting Whistleblowers with Access to Classified Information*, Oct. 10, 2012.
- B. Intelligence Community Inspector General, *External Review Panel Procedures Pursuant to Presidential Policy Directive - 19*, July 3, 2013.

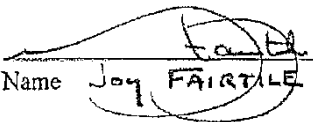
Agreement of the Parties.

For Facilities, Security and Contracting, by:

  
Name

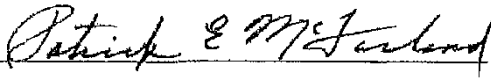
12-30-13  
Date

For the Personnel Security Appeals Board, by:

  
Name Joy FAIRTILE

1/10/14  
Date

For the Office of the Inspector General, by:

  
Name

12-19-13  
Date

MODIFICATION TO JANUARY 10, 2014 MEMORANDUM OF AGREEMENT  
BETWEEN FACILITIES, SECURITY AND CONTRACTING, THE  
PERSONNEL SECURITY APPEALS BOARD, AND THE OFFICE OF THE  
INSPECTOR GENERAL, U.S. OFFICE OF PERSONNEL MANAGEMENT ON  
ROLES AND RESPONSIBILITIES FOR IMPLEMENTING PRESIDENTIAL  
POLICY DIRECTIVE 19

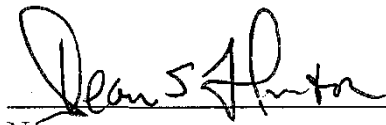
The parties to the Memorandum of Agreement (MOA) referenced above hereby modify the MOA's Limitations clause to read as follows, in accordance with the MOA's Modification clause:

Limitations.

This memorandum creates no legal rights and obligations. This memorandum must be implemented in accordance with applicable laws, rules, regulations, and presidential executive orders and directives, including, but not limited to, those governing the protection of classified national security information and intelligence sources and methods. This memorandum may be supplemented by other agreements, policies and procedures.

Agreement of the Parties.

For Facilities, Security and Contracting, by:

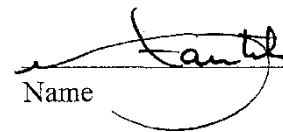


Name

3-12-14

Date

For the Personnel Security Appeals Board, by:

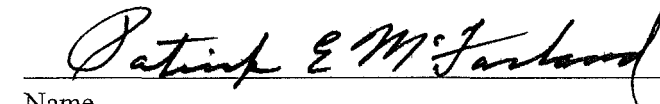


Name

3/12/14

Date

For the Office of the Inspector General, by:



Name

3-12-14

Date



**ATTACHMENT A**

October 10, 2012

PRESIDENTIAL POLICY DIRECTIVE/\_PPD-19

SUBJECT: Protecting Whistleblowers with Access to  
Classified Information

This Presidential Policy Directive ensures that employees (1) serving in the Intelligence Community or (2) who are eligible for access to classified information can effectively report waste, fraud, and abuse while protecting classified national security information. It prohibits retaliation against employees for reporting waste, fraud, and abuse.

To ensure the timely and effective implementation of the goals of this directive, I hereby direct that the following actions be taken:

A. Prohibition on Retaliation in the Intelligence Community

Any officer or employee of a Covered Agency who has authority to take, direct others to take, recommend, or approve any Personnel Action, shall not, with respect to such authority, take or fail to take, or threaten to take or fail to take, a Personnel Action with respect to any employee serving in an Intelligence Community Element as a reprisal for a Protected Disclosure.

Within 270 days of the date of this directive, the head of each Intelligence community Element shall certify to the Director of National Intelligence (DNI) 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 and that the review process is consistent with the requirements of this directive. Such review process shall apply to Personnel Actions that arise after the date on which the department or agency ("agency") head certifies the agency review process. If the head of any Intelligence Community Element fails to make this certification or if the DNI disagrees with the certification, the DNI shall notify the President.

The review process required by the above paragraph shall be consistent, to the fullest extent possible, with the policies and procedures used to adjudicate alleged violations of section 2302(b) (8) of title 5, United States Code. The review process shall provide for the protection of classified national security information and intelligence sources and methods. As part of the review process, the agency Inspector General shall conduct a

review to determine whether a Personnel Action violated this directive and may recommend that the agency take specific corrective action to return the employee, as nearly as practicable and reasonable, to the position such employee would have held had the reprisal not occurred. An agency head shall carefully consider the findings of and actions recommended by the agency Inspector General. To the extent authorized by law (including the Back Pay Act), corrective action may include, but is not limited to, reinstatement, reassignment, the award of reasonable attorney's fees, other reasonable costs, back pay and related benefits, travel expenses, and compensatory damages.

B. Prohibition on Retaliation by Affecting Eligibility for Access to Classified Information

Any officer or employee of an executive branch agency who has authority to take, direct others to take, recommend, or approve any action affecting an employee's Eligibility for Access to Classified Information shall not, with respect to such authority, take or fail to take, or threaten to take or fail to take, any action affecting an employee's Eligibility for Access to Classified Information as a reprisal for a Protected Disclosure.

Within 270 days of the date of this directive, the head of each agency in possession of classified information shall certify to the DNI, acting in his or her capacity as the head of the entity selected by the President under subsection 435b(b) of title 50, United States Code, and as the Security Executive Agent designated in Executive Order 13467 of June 30, 2008, that the agency has a review process that permits employees to appeal actions affecting Eligibility for Access to Classified Information they allege to be in violation of this directive and that the review process is consistent with the requirements of this directive. Such review process shall apply to actions that arise after the date on which the agency head certifies the agency review process. If the head of any agency fails to make this certification or if the DNI disagrees with the certification, the DNI shall notify the President,

The review process required by the above paragraph shall, to the fullest extent possible, be consistent with and integrated into the policies and procedures used to review security clearance determinations under Section 5.2 of Executive Order 12968 of August 2, 1995, as amended. The review process shall provide for the protection of classified national security information and intelligence sources and methods. As part of the review process, the agency Inspector General shall conduct a review to determine whether an action affecting Eligibility for Access to Classified Information violated this directive and may recommend that the agency reconsider the employee's Eligibility for Access to Classified Information consistent with the national security and with Executive Order 12968 and recommend that the agency take other corrective action to return the employee, as nearly

as practicable and reasonable, to the position such employee would have held had the reprisal not occurred. An agency head shall carefully consider the findings of and actions recommended by the agency Inspector General. To the extent authorized by law (including the Back Pay Act), corrective action may include, but is not limited to, reinstatement, reassignment, reasonable attorney's fees, other reasonable costs, back pay and related benefits, travel expenses, and compensatory damages,

C. Inspector General External Review Panel

An employee alleging a reprisal who has exhausted the applicable review process required by Section A or B of this directive may request an external review by a three-member Inspector General panel (External Review Panel) chaired by the Inspector General

of the Intelligence Community (on behalf of the DNI, acting in his capacity as the head of the entity selected by the President under subsection 435b(b) of title 50, United States Code, and as the Security Executive Agent designated in Executive Order 13467 of June 30, 2008). If such a request is made, the Inspector General of the Intelligence Community shall decide, in his or her discretion, whether to convene the External Review Panel, and, if so, shall designate two other panel members from the Inspectors General of the following agencies: Departments of State, the Treasury, Defense, Justice, Energy, and Homeland Security and Central Intelligence Agency. The Inspector General from the agency that completed the initial review shall not be a member of the External Review Panel. The External Review Panel shall complete a review of the claim, which may consist of a file review, as appropriate, within 180 days.

If the External Review Panel determines that the individual was the subject of a Personnel Action prohibited by Section A while an employee of a Covered Agency or an action affecting his or her Eligibility for Access to Classified Information prohibited by Section B, the panel may recommend that the agency head take corrective action to return the employee, as nearly as practicable and reasonable, to the position such employee would have held had the reprisal not occurred and that the agency head reconsider the employee's Eligibility for Access to Classified Information consistent with the national security and with Executive Order 12968.

An agency head shall carefully consider the recommendation of the External Review Panel pursuant to the above paragraph and within 90 days, inform the panel and the DNI of what action he or she has taken. If the head of any agency fails to so inform the DNI, the DNI shall notify the President.

On an annual basis, the Inspector General of the Intelligence Community shall report the determinations and recommendations and department and agency head responses to the DNI and, as appropriate, to the relevant congressional committees.

With respect to matters covered by this directive, all agencies shall cooperate with their respective agency Inspectors General, the Inspector General of the Intelligence Community, and External Review Panels and provide such information and assistance to their respective agency Inspectors General, the Inspector General of the Intelligence Community, and members of External Review Panels as such Inspectors General may request, to the extent permitted by law.

D. Policies and Procedures

Within 365 days of the date of this directive, the DNI shall, in consultation with the Secretary of Defense, the Attorney General, and the heads of agencies containing Intelligence Community Elements, issue policies and procedures for ensuring that all employees serving in Intelligence Community Elements are aware of the protections and review processes available to individuals who make Protected Disclosures. These policies and procedures shall to the extent practicable be publically available, and shall provide:

- (1) guidance for individual officers or employees regarding what disclosures are protected;
- (2) guidance for potential recipients on the appropriate handling of Protected Disclosures, including for referral by the DNI or Inspector General of the Intelligence Community to appropriate agency officials of any Protected Disclosures unrelated to national intelligence; and
- (3) information regarding the review processes required by Sections A, B, and C of this directive.

E. Review of Regulations Implementing Section 2303 of Title 5, United States Code

Within 180 days of the date of this directive, the Attorney General, in consultation with the Special Counsel and Federal Bureau of Investigation employees, shall deliver a report to the President that assesses the efficacy of the provisions contained in part 27 of title 28, Code of Federal Regulations in deterring the personnel practices prohibited in section 2303 of title 5, United States Code, and ensuring appropriate enforcement of that section, and describes any proposed revisions to the provisions contained in Part 27 of title 28 that would increase their effectiveness in fulfilling the purposes of section 2303 of title 5, United States Code.

F. Definitions

For purposes of this directive:

- (1) The term "Covered Agency" means an executive department or independent establishment, as defined under sections 101 and

104 of title 5, United States Code, that contains or constitutes an Intelligence Community Element, as defined below.

- (2) The term "Eligibility for Access to Classified Information" means the result of the determination whether an employee (a) is eligible for access to classified information in accordance with Executive Order 12968 (relating to access to classified information), or any successor thereto, and Executive Order 10865 of February 20, 1960, as amended (relating to safeguarding classified information with industry), or any successor thereto; and (b) possesses a need to know under such orders.
- (3) The term "Intelligence Community Element" means any executive agency or unit thereof determined by the President under section 2302(a)(2)(C)(ii) of title 5, United States Code, to have as its principal function the conduct of foreign intelligence or counterintelligence activities, including but not limited to the Office of the DNI, the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, and the National Reconnaissance Office. For purposes of this directive, the term "Intelligence Community Element" does not include the Federal Bureau of Investigation.
- (4) The term "Personnel Action" means an appointment, promotion, detail, transfer, reassignment, demotion, suspension, termination, reinstatement, restoration, reemployment, or performance evaluation; a decision concerning pay, benefits, or awards; a decision concerning education or training if the education or training may reasonably be expected to lead to an appointment, reassignment, promotion, or performance evaluation; a decision to order psychiatric testing or examination; and any other significant change in duties, responsibilities, or working conditions.

The term "Personnel Action" does not include the termination of an employee pursuant to section 1609 of title 10, United States Code. The term "Personnel Action" does not include the termination of an employee pursuant to section 102A(m) of the National Security Act of 1947, section 104A(e) of the National Security Act of 1947, or section 7532 of title 5, United States Code, so long as the official authorized by those provisions to terminate the employee (and not his or her delegee) (i) determines that the alternative legal procedures to terminate the employee cannot be invoked in a manner consistent with the national security and (ii) promptly notifies the Inspector General of the employing agency. The term "Personnel Action" does not include actions taken with respect to a position that the agency head has designated, prior to the action as being of a confidential, policy determining, policy making, or policy advocating character. The term "Personnel Action" does not include actions taken with respect to a member of the Armed Forces, as used in section 1034 of Title 10, United States Code.

The term "Personnel Action" does not include any actions taken prior to the issuance of this directive.

(5) The term "Protected Disclosure" means:

- (a) a disclosure of information by the employee to a supervisor in the employee's direct chain of command up to and including the head of the employing agency, to the Inspector General of the employing agency or Intelligence Community Element, to the Director of National Intelligence, to the Inspector General of the Intelligence Community, or to an employee designated by any of the above officials for the purpose of receiving such disclosures, that the employee reasonably believes evidences (i) a violation of any law, rule, or regulation; or (ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;
- (b) any communication described by and that complies with subsection (a)(1), (d), or (h) of section BH of the Inspector General Act of 1978 (5 U.S.C. App.); subsection (d)(5) (A) of section 17 of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403q); or subsection (k) (S)(A), (D), or (G), of section 103H of the National Security Act of 1947 (50 U.S.C. 403-Jh);
- (c) the exercise of any appeal, complaint, or grievance with regard to the violation of Section A or B of this directive;
- (d) lawfully participating in an investigation or proceeding regarding a violation of Section A or B of this directive; or
- (e) cooperating with or disclosing information to an Inspector General, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General,

if the actions described under subparagraphs (c) through (e) do not result in the employee disclosing classified information or other information contrary to law.

#### G. General Provisions

This directive shall be implemented in a manner consistent with applicable law, including all statutory authorities of the heads of agencies and Inspectors General, and does not restrict available rights, procedures, and remedies under section 2302(b) of Title 5, United States Code.

This directive is not intended to, and does not, create any right

or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA



UNCLASSIFIED//FOUO



INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY  
WASHINGTON, DC 20511

**IC IG EXTERNAL REVIEW PANEL PROCEDURES  
PURSUANT TO PRESIDENTIAL POLICY DIRECTIVE -19**

1. **(U) AUTHORITIES:** The National Security Act of 1947, as amended (50 U.S.C. § 403-3h et seq.); The Inspector General Act of 1978, as amended (5 U.S.C. App. § 7(a)&(c), SID; Intelligence Community Whistleblower Protection Act of 1998 (ICWPA), as amended (5 U.S.C. App. § 1); Executive Order 10865, as amended; Executive Order 12333, as amended; Presidential Policy Directive-19 (PPD-19): Protecting Whistleblowers with Access to Classified Information (October 10, 2012); and other applicable provisions of law and regulation.
2. **(U) REFERENCES:** Intelligence Community Directive 120: IC Whistleblower Protection.
3. **(U) PURPOSE:** These procedures set forth the Office of the Inspector General of the Intelligence Community (IC IG) responsibilities for processing employee requests for an external review process pursuant to Section C of PPD-19.
4. **(U) APPLICABILITY:** These procedures apply to any employee of a Covered Agency or any employee with access to classified information, alleging a reprisal, who has exhausted the applicable PPD-19 review procedures.
5. **(U) DEFINITIONS:** The following definitions from PPD-19 are incorporated here:
  - 1) "Covered Agency" means an executive department or independent establishment, as defined under sections 101 and 104 of title 5, United States Code that contains or constitutes an Intelligence Community Element, as defined below.
  - 2) "Intelligence Community Element" means any executive agency or unit thereof determined by the President under section 2302(a)(2)(C)(ii) of title 5, United States Code, to have as its principal function the conduct of foreign intelligence or counterintelligence activities, including but not limited to the Office of the DNI, the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, and the National Reconnaissance Office. For purposes of these procedures, the term "Intelligence Community Element" does not include the Federal Bureau of Investigation.

## IC IG External Review Panel Procedures

- 3) "Personnel Action" is defined as an appointment, promotion, detail, transfer, reassignment, demotion, suspension, termination, reinstatement, restoration, reemployment, or performance evaluation; a decision concerning pay, benefits, or awards; a decision concerning education or training if the education or training may reasonably be expected to lead to an appointment, reassignment, promotion, or performance evaluation; a decision to order psychiatric testing or examination; and any other significant change in duties, responsibilities, or working conditions. The term "Personnel Action" does not include:
- a. The termination of an employee pursuant to section 1609 of title 10, United States Code;
  - b. The termination of an employee pursuant to section 102A(m) of the National Security Act of 1947, section 104A(e) of the National Security Act of 1947, or section 7532 of title 5, United States Code, so long as the official authorized by those provisions to terminate the employee (and not his or her delegee):
    1. determines that the alternative legal procedures to terminate the employee cannot be invoked in a manner consistent with the national security, and
    2. promptly notifies the IG of the employing agency;
  - c. Actions taken with respect to a position that the agency head has designated, prior to the action as being of a confidential, policy determining, policymaking, or policy advocating character.
  - d. Actions taken with respect to a member of the Armed Forces, as used in section 1034 of Title 10, United States Code.
  - e. Any actions taken prior to the issuance of PPD-19.
- 4) "Eligibility for Access to Classified Information" is the result of the determination whether an employee (a) is eligible for access to classified information in accordance with Executive Order 12968 (relating to access to classified information), or any successor thereto, and Executive Order 10865 of February 20, 1960, as amended (relating to safeguarding classified information with industry), or any successor thereto; and (b) possesses a need to know under such orders.
- 5) "Protected Disclosure" is defined as:
- a. a disclosure of information by the employee to a supervisor in the employee's direct chain of command up to and including the head of the employing agency, to the Inspector General of the employing agency or IC element, to the DNI; to the IC IG; or to an employee designated by any of the above officials for the purpose of receiving such disclosures, that the employee reasonably believes evidences:
    - i. a violation of any law, rule, or regulation, or
    - ii. gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;
  - b. any communication described by and that complies with subsection (a) (1), (d), or (h) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App § I); subsection (d) (5) (A) of section 17 of the Central Intelligence Agency Act of 1949 (50 U.S.C. § 403q); or subsection (k) (5) (A), (D), or (G), of section 103H of the National Security Act of 1947 (50 U.S.C. § 403-3h);

## IC IG External Review Panel Procedures

- c. the exercise of any appeal, complaint, or grievance with regard to the violation of Section A or B of PPD-19;
- d. lawfully participating in an investigation or proceeding regarding a violation of Section A or B of PPD-19; or
- e. cooperating with or disclosing information to an Inspector General, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General.

Such disclosures will be protected if the action does not result in the employee making an unauthorized disclosure of classified information or disclosing other information contrary to law.

6. (U) POLICY: Presidential Policy Directive -19 (PPD-19) ensures that employees (1) serving in the Intelligence Community or (2) who are eligible for access to classified information can effectively report waste, fraud, and abuse while protecting classified national security information. It prohibits retaliation against employees for reporting waste, fraud, and abuse. Specifically, PPD-19 directs that:

- 1) Any officer or employee of a Covered Agency who has authority to take, direct others to take, recommend, or approve any Personnel Action, shall not, with respect to such authority, take or fail to take, or threaten to take or fail to take, a Personnel Action with respect to any employee serving in an Intelligence Community Element as a reprisal for a Protected Disclosure. (Section A) and
- 2) Any officer or employee of an executive branch agency who has authority to take, direct others to take, recommend, or approve any action affecting an employee's Eligibility for Access to Classified Information shall not, with respect to such authority, take or fail to take, or threaten to take or fail to take, any action affecting an employee's Eligibility for Access to Classified Information as a reprisal for a Protected Disclosure. (Section B).

As part of this policy, Section C of PPD-19 provides an external Inspector General (IG) review process for an employee, who has exhausted the applicable review process required by Section A or B, to seek review of reprisal actions that allegedly violate PPD-19. The procedures below outline the process for an employee seeking an IG external review and the process for conducting such a review.

7. (U//FOUO) PROCEDURES: Pursuant to Section C of PPD-19, an employee alleging a reprisal who has exhausted the applicable review process as required by PPD-19 may request an external review by a three-member IG panel chaired by the Inspector General of the Intelligence Community (IC IG).

A. Employee Request: An employee seeking an external review pursuant to Section C of PPD-19 shall provide a formal written request for such a review directly to the IC IG Hotline Manager within forty-five (45) calendar days of receiving an agency's final written disposition on his/her alleged reprisal complaint. Such request shall include:

- 1. Employee's Full Name
- 2. Federal Employing Agency
- 3. Reprisal Complaint, which should include a summary of:
  - i. Protected disclosure (s),
  - ii. Personnel actions, and/or Actions Affecting Eligibility for Access to Classified Information,

IC IG External Review Panel Procedures

- iii. Reprisal allegation(s),
- iv. Efforts to exhaust the applicable agency review process, and
- v. Agency final decision on the reprisal allegations.
4. Reason for seeking an external IG review, and
5. Any other supporting documentation.

B. IC IG Request Intake Process: Once the IC IG Hotline Manager receives a complete external review request package from a covered employee, the IC IG will:

1. notify the requesting employee that his/her request for review has been received and is under assessment;
2. notify the head of the department or agency where the employee is employed that the employee has made a request for an external review;
3. notify the IG who conducted the initial IG review that the employee has made a request for an external review;
4. request any and all official records, documents, materials, or accurate copies thereof from both the department or agency head and the IG who conducted the initial IG review; and
5. request a written certification from the department or agency that the requesting employee exhausted the applicable review process required under PPD-19.
6. To ensure that the IC IG's review includes the official agency record and can consider relevant materials in addition to those materials provided by the requesting employee, materials requested from the agency should be provided to the IC IG within two (2) weeks of the IC IG's request.
7. An agency employee's failure to provide requested materials in a timely manner, may result in administrative disciplinary action as stated in section 10 below.

## IC IG External Review Panel Procedures

- C. IC IG Initial Review: The IC IG will review all relevant materials submitted by the requesting employee, the head of the department or agency, and the IG who conducted the initial PPD-19 review. The IC IG will make a determination, based upon his or her discretion as outlined in IC IG guidance, whether to convene an external review panel (ERP) within forty-five (45) calendar days of receiving the requesting employee's complete external review request package. The IC IG will notify the requesting employee, the head of the employing agency, and the IG who conducted the initial IG review in writing of the determination to convene or not to convene an ERP.
- D. External Review Panel (ERP): If the IC IG determines to convene an external review panel, the IC IG will serve *as* the chair of the panel and will select two (2) other IGs from the Departments of State, Treasury, Defense, Justice, Energy, and Homeland Security and Central Intelligence Agency to serve on the ERP.
1. Within 180 calendar days of the ERP convening, the ERP shall review the reprisal allegations, which may consist of a file review of all relevant materials submitted, and will determine whether a violation of PPD-19 occurred and recommend corrective actions, if any. The ERP will apply general acceptable standards of review to the reprisal allegations including, but not limited to:
    - i. Title 5, and applicable case law, in so far as possible;
    - ii. Council of the Inspectors General on Integrity and Efficiency, Quality Standards for Investigations (2011);
    - iii. Directives, instructions and other regulations of the originating agency.
  2. The IC IG will notify the requesting employee, the head of the employing Department or agency, and the agency IG in writing of the determination.
  3. The IC IG will provide any of the ERP's recommendations for corrective action to the head of the employing agency, which may include corrective action to return the employee, as nearly as practicable and reasonable, to the position such employee would have held had the reprisal not occurred and that the department or agency head reconsider the employee's Eligibility for Access to Classified Information consistent with the national security and with Executive Order 12968.
  4. To avoid conflicts of interest and protect the objectivity of the ERP, none of the listed ERP IGs may serve on an ERP for a reprisal allegation that they reviewed previously as part of a PPD-19 review process or other IG review process. (See section 7.E for ODNI Employees).
- E. ODNI Employee Request for an ERP. The IC IG will conduct the initial IG review for ODNI employees who allege reprisal in violation of PPD-19 and therefore will be recused from the ERP proceedings. When an ODNI employee requests an ERP as outlined in Section 6.A above, one of the other IGs from the Departments of State, Treasury, Defense, Justice, Energy, and Homeland Security and Central Intelligence Agency will be selected on a rotating basis *to* conduct the initial review and make the determination to convene an ERP. If the selected IG determines to convene an ERP, the selected JG will serve as the ERP panel chair and execute the IC IG actions outlined in Section 7.D above.

IC IG External Review Panel Procedures

8. **(U) DEPARTMENT OR AGENCY HEAD ACTION:** The department or agency head shall carefully consider the recommendation for corrective action, if any, of the ERP pursuant to the Section 7. Within ninety (90) calendar days, the department or agency head shall inform the ERP, and the DNI of what action he or she has taken regarding the ERP's recommendation. If the department or agency head fails to so inform the DNJ, the DNI shall notify the President.
9. **(U) IC IG ANNUAL REPORT:** On an annual basis, the IC IG shall report the ERP determinations and recommendations and department and agency head responses to such recommendations to the DNI and, as appropriate, to the relevant congressional committees.
10. **(U) COOPERATION WITH IGs:** With respect to matters covered by these procedures, all agencies shall cooperate with their respective agency IGs, the IC IG, and ERPs and provide such information and assistance to their respective agency IGs, the IC IG, and ERPs as such IGs may request, to the extent permitted by law.
11. **(U) EFFECTIVE DATE:** These Procedures are effective upon signature.

  
\_\_\_\_\_  
I. Charles McCullough, III  
Inspector General of the Intelligence Community

07-03-2013  
Date