Protecting Whistleblowers with Access to Classified Information

Welcome to the Protecting Whistleblowers with Access to Classified Information Training
The Protecting Whistleblowers with Access to Classified Information Course is a four-part training curriculum that satisfies the requirements of Presidential Policy Directive-19 (PPD 19) to ensure that all Executive Branch employees and contractors are aware of protections for whistleblowers eligible for access to classified information.

- Module 1 of this training applies to all executive branch agency employees and contractors eligible for access to classified information and provides fundamental information on whistleblowing and available protections.
- Module 2 of this training applies to all executive branch agency employees and contractors eligible for access to classified information and addresses retaliatory adverse security clearance actions.
- Module 3 of this training applies to all employees of Intelligence Community (IC) elements and addresses retaliatory adverse personnel actions against IC whistleblowers.
- Module 4 of this training applies to all executive branch agency employees in supervisory positions with access to classified information and addresses best practices for managers and supervisors.

This training ensures that personnel eligible for access to classified information can effectively report illegality, waste, fraud, and abuse while protecting classified national security information. This training covers the process for making Protected Disclosures and protections and review processes available to individuals who report Protected Disclosures. This training also highlights best practices for managers and supervisors. This training is limited to protections available for whistleblowers with access to classified information under PPD-19 and the National Security Act. For non-IC personnel, this training is supplemental to agency-specific whistleblower training materials and resources. For questions about other whistleblower protections, please contact **[insert Agency-specific POC phone number, email address or website]**

MODULE 1

SCOPE OF MODULE 1 – Whistleblower Fundamentals
This module applies to all Executive Branch employees and contractors and provides fundamental information concerning whistleblower procedures and protections.

LESSON 1: INTRODUCTION

What Would You Do?
In organizations of all sizes and sectors, fraud, waste, and abuse are unfortunate realities. You may have read about wrongdoing or seen it in the news, but what would you do if you witnessed it firsthand? What if you had a reasonable belief but figured you couldn't prove it, or worse, that you should say something, but don't want to be seen as a troublemaker?

Imagine, however, that you reasonably believed a classified program violated the law. What if you participated in the program or your direct supervisor managed the program? Do you think you would feel compelled to report the allegation?

You're Not Alone
If you don't know what you would or should do in these situations, you're in good company. Most government employees and contractors haven't spent much time considering how to report fraud, waste, abuse, or illegality, or what to do if they suffer consequences for speaking out. The stress of suspecting wrongdoing but not knowing what to do can be a considerable burden on anyone. Whistleblowers often talk about their conflicting feelings, doubts, and fears that go along with not knowing the answer to "Now what?"

The good news is that you have allies to help you through every step of the process. There are experts in whistleblower laws, protections, and resources at your disposal. Knowing those laws and protections—and more importantly, how to access them—will prepare you in the event you witness something you must report.

Why do we blow the whistle?
Every Federal employee and government contractor has the right and responsibility **[pop-up]** to report truthful allegations of wrongdoing in accordance with specific legal processes. Further, whistleblowing is critical to national security and the mission of the Federal government because it:

- Saves taxpayers millions of dollars each year.
- Serves the public interest by ensuring that the Federal government remains an ethical and safe workplace.
- Allows human, technical, and financial resources to be targeted at fixing the problem.
- Protects the public's health, welfare, and safety.

Pop-up: The following resources provide rights and responsibilities pertaining to whistleblowing:
- 5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch
- Executive Order 12674, Principles of Ethical Conduct for Government Officers and Employees
- PPD-19, Protecting Whistleblowers with Access to Classified Information

- Intelligence Community Directive 120 (ICD 120), Intelligence Community Whistleblower Protection
- Principles of Professional Ethics for the Intelligence Community

LESSON 2: PROCEDURES FOR PROTECTED DISCLOSURES INVOLVING CLASSIFIED INFORMATION

What is a whistleblower and what do they report?

A whistleblower is an employee or contractor who reports to authorized individuals certain classified and unclassified matters that involve:

- A violation of any law, rule, or regulation.
- Gross mismanagement.
- A gross waste of funds.
- An abuse of authority.
- A substantial and specific danger to public health and safety.

As a reminder, you always have an obligation to protect classified information. It is unlawful to disclose classified information to any unauthorized entity (for example, the media, non-government organizations), even if the information is not marked as classified. Making an unauthorized disclosure of classified information does not constitute whistleblowing nor is it an act of free speech. Like any mishandling of classified information, unlawful disclosures may subject you to potential criminal prosecution, civil penalties, and administrative disciplinary action.

What are Protected Disclosures?

Protected Disclosures are disclosures of information to authorized officials that the employee reasonably believes evidences a violation of law, rule, or regulation; or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

For whistleblowers with access to classified information, protected disclosures also include:

- Communications of an "urgent concern" **[pop-up]** to your agency's Inspector General (IG), the Inspector General for the Intelligence Community (IC IG), or congressional intelligence committees;
- Participation in an IG audit, inspection, or investigation;
- Participation in an investigation or proceeding regarding an alleged reprisal for a Protected Disclosure; and
- Exercising any appeal, complaint or grievance regarding alleged reprisal for a Protected Disclosure.

We all have a responsibility to report wrongdoing through Protected Disclosures.

Pop-up: Communications of "Urgent Concern" include:

- A serious or flagrant problem, abuse, violation of law or Executive Order, or deficiency relating to the funding, administration, or operations of an intelligence activity involving classified information, but does not include differences of opinions concerning public policy matters.
- A false statement to Congress, or a willful withholding from Congress, on an issue of material fact relating to the funding, administration, or operation of an intelligence activity.
- Reprisal or threat of reprisal in response to an employee's reporting an urgent concern.

Note: Personnel who intend to report to congressional intelligence committees must follow specific reporting procedures. For detailed information concerning reporting to Congress, please contact the IC IG or view the summary of procedures described on the IC IG website **[insert link to: https://www.dni.gov/index.php/about-this-site/contact-the-ig/how-to-file-a-whistleblower-complaint]**.

To whom do I report wrongdoing?

Personnel have many options for making a Protected Disclosure, several of which do not require going through your chain of command. They include:

- Your supervisor;
- Personnel in your direct chain of command up to and including your agency head;
- The Director of National Intelligence (DNI);
- Your agency's IG, via HOTLINE phone, email, or in person...you can report anonymously;
- The Office of the Inspector General for the Intelligence Community (IC IG);
- A congressional intelligence committee or member of a congressional intelligence committee consistent with specific reporting procedures summarized on the IC IG website [insert link to: https://www.dni.gov/index.php/about-this-site/contact-the-ig/how-to-file-a-whistleblower-complaint]; and
- Other officials designated to receive Protected Disclosures. Depending on the nature of the allegation, these designated officials may include other compliance offices, such as your agency's Equal Employment Office (EEO), Office of General Counsel (OGC), your Intelligence Oversight (IO) officer, or your agency's (or ODNI's) Office of Civil Liberties, Privacy, and Transparency (CLPT).

If unsure, personnel are encouraged to contact their agency's IG **[insert link to Agency IG website]** or the IC IG **[insert link to: https://www.dni.gov/index.php/about-this-site/contact-the-ig]**.

Do policy disputes, analytic disagreements, or technical dissents qualify as wrongdoing?

Only violations of law, rule, or regulation, or fraud, waste, and abuse qualify as wrongdoing for purposes of making a Protected Disclosure. Wrongdoing is easy to confuse with the following situations, none of which require reporting:

- A policy dispute, such as program funding priorities not required by law.
- Analytic disagreements, short of a deliberately misleading or factually incorrect assessment. Agency programs, such as an Analytic Ombudsman, address analytic disputes.
- Technical dissent on the capability or capacity of a system, weapon, or program.

However, a dispute over a policy's constitutionality or legality could be reportable as a Protected Disclosure.

How do I get the information that supports my allegations to the right people?

Take the following steps when you have something to disclose:

- **Jane/John Doe.** Decide whether you want to maintain confidentiality *before* you report the wrongdoing.
- **Do research.** Do your best to identify the law, rule, and/or regulation you think was or is being violated.

- **Be succinct.** Prepare an organized summary of the facts that lists what you witnessed and what law, rule, and/or regulation you believe it violates.
- **Provide helpful information.** End your summary with any contact information you have for potential witnesses and the location of any relevant hard and soft copy data of which you are aware that may support your allegations.
- **Document it.** Keep a record of your disclosure to include the subject, date, time, and those persons to whom you made it.
- **Protect it.** Lawfully handle all information in accordance with its classification and privacy restrictions and ensure that you disclose the information to an individual or organization with the requisite security clearance. If you need to disclose classified information to make a disclosure, notify the recipient of that so they can make sure that appropriate procedures are in place before you make any disclosure of classified information.

What if I just need basic policy or procedural guidance on an issue I have concerns about?
Contact your agency's IG or the IC IG. They can help identify policies or statutes that will help you determine if a specific law has been violated, prepare you for the whistleblowing process (if necessary), and what oversight body can best help you.

How realistic is it that I'll maintain my confidentiality?
IG investigators, auditors, evaluators, and inspectors make every effort to protect your identity, but they cannot guarantee complete confidentiality. At some point in an inquiry, it may be necessary to reveal your identity to further the whistleblowing process or as otherwise required by law. Additionally, depending on the nature of the inquiry, the information disclosed may make your identity obvious despite all precautions taken to maintain your confidentiality. The office receiving your complaint will explain exactly what they do to maintain your confidentiality. As tempting as it is, you probably will want to avoid discussing your whistleblowing with anyone outside the reporting process. If you do, you risk revealing your identity.

Why isn't what I reported being investigated? After what I disclosed, surely the IG would have looked into it.
This is often the hardest part for whistleblowers—eagerly anticipating corrective action to occur, yet seemingly nothing happens at all. Investigators may be under statutory or professional obligations to not share information with you. Moreover, they are deliberately discreet to avoid disrupting the workplace and to encourage employees' willingness to come forward. The sensitive nature of investigations is such that you often don't know they're occurring.

How do we meet our whistleblowing obligations without triggering an insider threat concern?
Although they may seem at odds with one another, whistleblowing and insider threat missions share the same goal—to root out and correct deficiencies within the Federal government. So long as you report through one of the appropriate channels available to you, the documentation that results from this whistleblowing process protects you from the appearance of insider threat activity.

KNOWLEDGE CHECK: QUESTION 1
Choose the statements that are true about whistleblowing (Select all that apply):
A. It doesn't apply to contractors.
B. It is optional if I think it might embarrass agency leadership.
C. Whistleblowing is a responsibility of government employees.
D. Describes the lawful process for reporting wrongdoing such as fraud, waste, or abuse.

E. It includes reporting policy and analytic disputes in my office.

Correct/Incorrect Feedback: C and D are correct. Whistleblowers include both government employees and contractors who follow the specific lawful process for reporting wrongdoing. Whistleblowing is everyone's responsibility, even if it may be embarrassing to your agency, but does not include policy or analytic disputes. Note: as discussed further in this training, PPD-19 provides different protections for employees and contractors. Whistleblower protections against adverse personnel actions under PPD-19 do not apply to contractors.

KNOWLEDGE CHECK: QUESTION 2

You can report wrongdoing involving classified information to (Select all that apply):

A. The IC IG Hotline.
B. Your local IG's Hotline.
C. Your supervisor in most cases.
D. The Director of National Intelligence
E. A non-government organization or member of the media.

Correct/Incorrect Feedback: You can report wrongdoing to the IC IG Hotline, your local IG, your supervisor in most cases, or the DNI. Classified information must still be reported using secure lines of communication. Reporting classified information to the media or an unauthorized organization is an unlawful disclosure—a leak—that exposes you to potential criminal prosecution.

KNOWLEDGE CHECK: QUESTION 3

Read the following scenario and answer the question on the following page.

Denise tells her co-worker, Adam, she just completed a new classified report for their supervisor, Mr. Snyder. Denise also confides to Adam that Mr. Snyder deliberately revised portions of her analysis with false information to mislead leadership. Adam is surprised, but Denise says Mr. Snyder has done this with a previous classified report as well. Adam considers contacting a media outlet to raise concerns that his agency has been misleading government officials with falsified classified reports.

Regarding the scenario you just read, which of the following statements are true? (Review the scenario by clicking on the Scenario button to the right.)

A. Adam can share classified information with the reporter to discuss what's going on in his office so long as he stays "off the record."
B. Adam can include classified information when venting his frustration via a public blog site so long as he does so anonymously.
C. Because Adam has good reason to believe that misconduct is occurring in his work unit, he is required to report this misconduct.
D. In order to comply with agency policies, Adam must first report his suspicions to his immediate supervisor.
E. Adam can report his suspicions to an IG Hotline and remain anonymous.

Correct/Incorrect Feedback: Only C and E are true.

LESSON 3: BETTER POLICY, CONSISTENT PROTECTIONS

A Tradition of Whistleblowing

In 1778, whistleblowing formally became part of the future Federal Government mission when the Continental Congress made it our duty. Today, Executive Order (EO) 12674, and related laws and policies covered later in this course, continue the tradition the Continental Congress legislated more than two centuries ago. Combined, these statutes and policies set the standards of conduct for all Executive Branch employees and contractors, including our requirement to blow the whistle on waste, fraud, abuse, and violations of U.S. laws and regulations.

> **Pop-up: Excerpted from Journals of the Continental Congress, 1774-1789:**
> On July 30, 1778, the members of the Continental Congress unanimously enacted the first whistleblower legislation in the United States that read:
>
> > "Resolved, That it is the duty of all persons in the service of the United States, as well as all other the inhabitants thereof, to give the earliest information to Congress or other proper authority of any misconduct, frauds or misdemeanors committed by any officers or persons in the service of these states, which may come to their knowledge."
>
> Additionally, the Founding Fathers understood the demand they were placing on civil servants, so they included in the legislation a provision for legal expenses in the event whistleblowers were retaliated against.

Safeguards for Everyone

Fast forward from 1778 to 2012 when President Obama issued Presidential Policy Directive-19 (PPD-19), "Protecting Whistleblowers with Access to Classified Information." **[insert link to: https://www.whitehouse.gov/sites/default/files/image/ppd-19.pdf]**

> **Pop-up: Presidential Policy Directives (PPDs):** PPDs provide specific, mandatory direction to Federal government agencies.

Under PPD-19, for the first time, whistleblowers with access to classified information received protections against reprisal for reporting fraud, waste, abuse, and illegality. More specifically, PPD-19 prohibited the following:

- Actions affecting eligibility for access to classified information as a reprisal against all Executive Branch employees and contractors for a Protected Disclosure; and
- Adverse personnel actions as a reprisal against IC employees for a Protected Disclosure (discussed in Module 3 of this training).

Statutory Protections

In 2014, whistleblowers received overarching statutory protections from retaliatory security clearance actions. The National Security Act, as amended in 2014, now prohibits retaliatory revocation of security clearances and access determinations from being used as reprisal against Federal employees and contractors who make lawful disclosures of fraud, waste, abuse, or illegality. Additionally, the National Security Act was amended to prohibit adverse personnel actions against IC employees who make Protected Disclosures (discussed in Module 3). The amendments to the National Security Act do not protect contractors against adverse personnel actions.

For IC employees, these new provisions provided the first clear statutory protections from reprisal for blowing the whistle. Previous statutory whistleblower protections, like the Whistleblower Protection Act of 1989, the Whistleblower Protection Enhancement Act of 2012, and the Intelligence Community

Whistleblower Protection Act, either specifically excluded IC employees from protections or only protected classified information, not employees.

These provisions also created new protections for all Executive branch employees and contractors eligible for access to classified information to engage in whistleblowing while also ensuring that classified information remains safeguarded.

Let the Experts Help

Understanding statutes and regulations can be tedious, but they are central to helping you know when and how to blow the whistle. Rules and laws define the work we do, so if you're not familiar with the ones that govern the IC, you can easily mistake a policy disagreement for wrongdoing. This is why it's critical to take your concerns to those who can help you determine what steps, if any, to take when you believe your information may warrant reporting. Your agency's IG or the IC IG may be available to guide you through the steps to properly report wrongdoing or direct you to someone who can.

KNOWLEDGE CHECK: QUESTION 4

Which of the following is true (Select all that apply):

A. PPD-19 protects both employees and contractors from retaliatory security clearance actions.
B. Until 2012, the Federal government historically did not recognize the importance of whistleblowers.
C. Agency's IG or Office of General Counsel can provide additional information on whistleblower protections.
D. PPD-19 and the National Security Act protect employees who disclose classified information to the media from adverse security clearance actions.

> **Correct/Incorrect Feedback**: A and C are true. The Federal government has recognized the importance of whistleblowers since its founding, but only recently provided whistleblower protections against adverse security clearance actions through PPD-19. PPD-19 and the National Security Act only provide protections for employees who report wrongdoing to authorized individuals through the Protected Disclosure process. PPD-19 and the National Security Act do not provide contractors with protections against adverse personnel actions. Personnel are encouraged to contact the agency's IG or OGC for guidance.

MODULE 2

SCOPE OF MODULE 2 – PROTECTING WHISTLEBLOWERS AGAINST RETALIATORY ADVERSE SECURITY CLEARANCE ACTIONS

This module applies to all Executive Branch employees and contractors and addresses protections against adverse security clearance or other actions affecting eligibility for access to classified information as reprisal for a Protected Disclosure.

This Module does not cover whistleblower protections against adverse personnel actions.

- For agencies outside the IC, please refer to your agency's training materials and resources concerning whistleblower protections against adverse personnel actions.
- For IC employees, please complete this training module and then continue to Module 3 for IC-specific training concerning whistleblower protections against adverse personnel actions.

LESSON 1: REFRESHER

Recap of Module 1

In Module 1 of this training, we learned the following:

- What is and what is not whistleblowing
- How to make a Protected Disclosure
- Protections against retaliatory security clearance and personnel actions under Presidential Policy Directive-19 (PPD-19) and the National Security Act

LESSON 2: ESTABLISHING REPRISAL

Blowing the whistle internally is an act of patriotism.

That's right – whistleblowing is a professional responsibility that every employee is obliged to uphold. Truth, lawfulness, integrity, and stewardship are bedrock values that have defined the Federal Government's ethical code for decades. Every employee is responsible to report wrongdoing through appropriate channels. Further, every supervisor and management official is responsible to encourage and support an employee's professional duty to blow the whistle when the situation calls for it. It's equally important to demonstrate respect for the courage and professionalism it takes to report wrongdoing.

What security clearance actions constitute reprisal?

Federal government officers or employees may not take, fail to take, or threaten to take any action affecting an employee's security clearance, including the denial, suspension, or revocation of a clearance, or eligibility for access to classified information for reporting wrongdoing. If an official takes an action that affects an employee's security clearance or eligibility for access to classified information, then it is critical that the official, on a thoroughly independent basis, state the rationale for the security clearance action.

Determining reprisal

Although proving reprisal can be complex, it starts with three simple questions:

1) Did the individual make a Protected Disclosure?
2) Was an action affecting the individual's eligibility for access to classified information taken after the Protected Disclosure?
3) Was the Protected Disclosure a contributing factor in the decision to take the security clearance action? This is often established by determining if the official affecting the individual's eligibility for access to classified information had knowledge of the disclosure and if the official thereafter took an improper action affecting the employee's security clearance or eligibility to access to classified information (also known as the "knowledge and timing test").

Determining reprisal *(continued)*

An IG investigator will see if an adverse action was improper by assessing whether the official would have taken the same adverse action absent the employee blowing the whistle. The investigator will review all the evidence and determine if the reprisal claim has merit.

When supervisors follow the proper policies and procedures, document their decision making process, and treat employees with fairness, any adverse actions they take for appropriate reasons will likely be found as legitimate rather than reprisal. However, supervisors who fail to follow agency regulations and

don't accurately and thoroughly document their employees' performance or non-whistleblowing related conduct will lack the evidence they need to clear themselves and the agency of reprisal allegations.

Knowledge: In order to establish prohibited reprisal, the person taking the action affecting the security clearance or eligibility for access to classified information must have knowledge of the Protected Disclosure. Whether the official had knowledge that the employee reported wrongdoing is essential to proving reprisal. An official can have knowledge in two ways:

- **Direct.** Evidence that shows the official *directly knows* the employee made a disclosure. For example, the employee included the official on an email to the IC Hotline.
- **Imputed** (also called *Constructive*). Think of this as "unwitting inheritance and implementation." For example, a departing supervisor left his successor an adverse action to implement against an employee. He did not to tell his successor his recommendation for the adverse action was unfounded or that the employee made a protected disclosure. The new supervisor fails to verify the departing supervisor's claims and implements the adverse action, unwittingly (constructively) reprising against the employee.

Action Affecting Eligibility for Access to Classified Information: There must have been an action affecting the employee's eligibility for access to classified information, most commonly, an adverse security clearance action. Although eligibility for access to classified information alone is not a direct source of pay and benefits, it is required for employment in the IC and for various jobs in many Federal agencies. This applies to both government and contractor employees.

So, am I protected from the adverse security clearance action?
Imagine we've determined the supervisor has knowledge of the employee's disclosure and took adverse action. However, just as every workplace communication is not a Protected Disclosure, not every adverse action a supervisor or security official takes is a prohibited reprisal. Whistleblowing laws protect legitimate adverse security clearance actions if the agency demonstrates that it would have taken the same action in the absence of a Protected Disclosure.

Whistleblowers may seek the advice of any one of the oversight bodies identified in this training to further help you understand the rules addressing reprisal before any potential adverse action is taken.

KNOWLEDGE CHECK: QUESTION 1
The following actions, based on actual cases, were taken against employees who made protected disclosures known to their supervisors. Which of the following scenarios are potential retaliatory actions (select all that apply)?
A. Lisa's security clearance is suspended after her checking account is overdrawn. Three of her immediate peers have had overdrafts in the past year and their security clearance status remained unchanged.
B. Mark's agency indicated he has no "need to know" and has restricted his access to information he needs to successfully complete his performance objectives. No other employee in his work group has had a declined NTK determination in several years, and there was no change in Mark's functions that would have changed his need to know.
C. Special Agent Smith "pulled his badge" during a routine traffic stop where his passenger was a prostitute. As a result, he is now the subject of a Limited Access Authorization that reduced his access to classified information.

Correct feedback: A and B are correct. Treating employees in a manner different from their peers in the same or similar situations following a protected disclosure is strong evidence of retaliatory actions.
Incorrect feedback: C is incorrect. This is a justified personnel action.

KNOWLEDGE CHECK: QUESTION 2
Read the following scenario and determine whether it's true or false that Andrew reprised against his employee.
Andrew becomes the acting supervisor of an employee with a successful performance history who made a Protected Disclosure during the previous manager's tenure. The previous manager knew the employee blew the whistle, but Andrew does not. Based on the outgoing manager's recommendation, Andrew refers derogatory information to a central adjudication facility leading to the suspension of the employee's security clearance.
Which of the following is true (select all that apply):
A. Andrew did not engage in prohibited reprisal because he had no knowledge of the employee's previous Protected Disclosure.
B. Andrew engaged in prohibited reprisal because he had implied (or constructive) knowledge of the employee's previous Protected Disclosure.
C. Andrew did not engage in prohibited reprisal because the employee did not suffer an action affecting eligibility for access to classified information.
D. Andrew engaged in prohibited reprisal because the employee did suffer an action affecting eligibility for access to classified information.

Correct/Incorrect Feedback: B and D are correct. Andrew had implied (or constructive) knowledge of the Protected Disclosure because he followed the previous supervisor's recommendations without independently confirming the claims. Also, Andrew's action constitutes an adverse security clearance action because it affected the employee's eligibility for access to classified information.

KNOWLEDGE CHECK: QUESTION 3
Read the following scenario and determine whether it's true or false that the supervisor reprised against Rita.
Rita reports to her supervisor that a classified program is violating agency regulations. Her supervisor then refers Rita to a central adjudication facility leading to the suspension of her security clearance.

Which of the following is true (select all that apply):
A. The supervisor did not engage in prohibited reprisal because Rita did not make a Protected Disclosure.
B. The supervisor did not engage in prohibited reprisal because the supervisor did not personally suspend her security clearance.
C. The supervisor did engage in prohibited reprisal because Rita made a Protected Disclosure and the supervisor took an action adversely affecting Rita's eligibility for access to classified information.

Correct/Incorrect Feedback: C is correct. Rita properly followed the Protected Disclosure process by reporting wrongdoing to her supervisor and her supervisor had direct knowledge of Rita's Protected Disclosure. The supervisor's action constitutes an adverse security clearance

action because the referral to the central adjudication facility affected Rita's eligibility for access to classified information.

LESSON 3: WHAT NEXT? REPRISAL REVIEW PROCESSES AND REMEDIES

Filing a Reprisal Complaint

Under PPD-19, each Executive branch agency in possession of classified information certified to the DNI that it has a review process that permits employees and personnel to appeal actions affecting eligibility for access to classified information that they believe to be reprisal for Protected Disclosures. The review process requires that the agency's IG conduct a review to determine whether a security clearance action constitutes prohibited reprisal for a Protected Disclosure.

Appealing a Security Clearance Action

Under the National Security Act, as amended in 2014, personnel who believe they have been subjected to prohibited reprisal may appeal the adverse security clearance decision with the agency within 90 days after the issuance of the notice of the decision.

Personnel should contact their agency's IG to answer questions about their agency's specific personnel policies, provide procedural guidance, and otherwise assist in filing a complaint concerning alleged prohibited reprisal.

Agency IG Findings

Based on the IG investigation results, the agency IG 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. The agency head is not required to follow the IG's recommendations but is required to carefully consider the IG's findings and recommended actions.

Remedies Available

To the extent authorized by law, 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. This is in addition to other remedies that may be available under other anti-retaliation laws.

What if the agency IG does not find that there has been reprisal?

Under PPD-19, after exhausting the agency's review process, personnel have an opportunity to request a review of their reprisal claim by an External Review Panel, which is chaired by the IC IG. The IC IG has the discretion to decline requests for appeal; however, if the request is accepted, the External Review Panel, consisting of the IC IG and two other OIGs who were not previously involved in reviewing the matter selected by the IC IG from a list in PPD-19, will complete the review within 180 days of accepting the appeal.

What should I expect from the External Review Panel?

If the External Review Panel determines that the individual was the subject of a prohibited reprisal for a Protected Disclosure, 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. The agency head is not required to follow the panel's recommendations

but must carefully review the panel's recommendation and, within 90 days, inform the panel and the DNI of the action taken.

KNOWLEDGE CHECK: QUESTION 3

Which of the following is true (select all that apply):

A. Each Executive Branch agency with access to classified information has a review process allowing the agency's IG to determine whether an action affecting eligibility for access to classified information constitutes a prohibited reprisal.

B. The agency head is required to take all corrective actions recommended by the IG.

C. If the agency's IG does not find that there has been prohibited reprisal, the employee has no further recourse to review a reprisal claim.

D. Corrective action is limited to reinstatement.

> **Correct/Incorrect Feedback**: Only A is true. Personnel should review their own agency's personnel policies and review processes for allegations of reprisal. The agency head is only required to consider all of the IG's findings and recommended action, and retains the ultimate authority with regard to the classification action consistent with agency policies. If the agency OIG does not find reprisal, the individual may request a review of the reprisal claim with an External Review Panel. Corrective actions are not limited to reinstatement – they also include reassignment, reasonable attorney's fees, other reasonable costs, back pay and related benefits, travel expenses, and compensatory damages.

MODULE 3

SCOPE OF MODULE 3 – IC WHISTLEBLOWER PROTECTIONS AGAINST RETALIATORY ADVERSE PERSONNEL ACTIONS

Module 3 of this training covers whistleblower protections for IC employees against adverse personnel actions as a reprisal for a Protected Disclosure under PPD-19. This module applies only to employees of IC elements. Contractors within the IC are not protected against retaliatory adverse personnel actions under PPD-19, but do have whistleblower protections concerning retaliatory actions affecting security clearances or eligibility for access to classified information (as discussed in Module 2 of this training).

LESSON 1: REFRESHER

Recap of Modules 1-2

In Modules 1-2 of this training, we learned the following:

- What is and what is not whistleblowing
- How to make a Protected Disclosure
- Whistleblower protections under Presidential Policy Directive-19 (PPD-19) and the National Security Act
- Establishing allegations of prohibited reprisal in the form of adverse security clearance actions
- Review processes and remedies for prohibited retaliatory security clearance actions

LESSON 2: IC PROTECTIONS AGAINST RETALIATORY PERSONNEL ACTIONS

IC Protections against retaliatory personnel actions

As discussed in Module 1, in 2012, the President issued PPD-19, "Protecting Whistleblowers with Access to Classified Information." PPD-19 prohibited the following:

- Adverse security clearance actions as a reprisal against all Executive Branch employees and contractors for a Protected Disclosure; and
- Adverse personnel actions as a reprisal against IC employees for a Protected Disclosure.

In 2014, as directed by the President in PPD-19, the DNI issued Intelligence Community Directive 120 (ICD 120), "IC Whistleblower Protection." **[insert link to https://www.dni.gov/files/documents/ICD/ICD%20120.pdf]**

> **Pop-up: Intelligence Community Directives (ICDs):** The DNI issues ICDs to establish policy and provide direction to the IC.

ICD 120 outlines how the IC will implement PPD-19. It requires IC elements to use workforce communications and training (you're taking it) to ensure that we all understand the process for making a protected disclosure about illegality, waste, fraud, or abuse. It also details our protections from reprisal and the reprisal review process, covered later in this training.

Also in 2014, the National Security Act was amended to prohibit adverse personnel actions from being used as reprisal against IC employees who make lawful disclosures of fraud, waste abuse, or illegality. For IC employees, these new provisions provided the first clear statutory protections from reprisal for blowing the whistle. Previous statutory whistleblower protections, like the Whistleblower Protection Act of 1989 or the Intelligence Community Whistleblower Protection Act, either specifically excluded IC employees from protections or only protected classified information, not employees.

What do these new protections prohibit?
PPD-19 and the National Security Act, as amended, prohibit any officer or employee from taking or failing to take, or threatening to take or fail to take, a personnel action against an IC employee as a reprisal for a Protected Disclosure.

What are personnel actions?
Personnel actions may include a promotion, demotion, detail, transfer, termination, suspension, performance evaluation, or any other significant change in duties, responsibilities, or working conditions.

KNOWLEDGE CHECK: QUESTION 1
Which of the following is true (select all that apply):
A. PPD-19 and the National Security Act protect both IC employees and contractors from retaliatory adverse personnel actions.
B. Until 2012, IC employees did not have protections from reprisal for whistleblowing.
C. ICD 120 defines how the IC will implement PPD-19.
D. ICD 120 applies to all Executive branch agencies.

> **Correct/Incorrect Feedback**: B and C are true.

KNOWLEDGE CHECK: QUESTION 2
Which of the following would NOT be considered a personnel action:
A. Denial of a promotion
B. Negative performance evaluation
C. Significant change in duties

D. Receiving a text message from a supervisor at 3 a.m. concerning an overdue assignment

Correct/Incorrect Feedback: D is not a personnel action.

LESSON 3: ESTABLISHING REPRISAL

What adverse personnel actions constitute a reprisal?
A Federal Government supervisor may not take, fail to take, or threaten to take any personnel action against an employee because of a Protected Disclosure. To determine whether an action is adverse, the first and simplest question is: "Will this action adversely affect the employee's pay or benefits?" If the answer is yes, it's critical the supervisor, on a thoroughly independent basis, state their rationale for the adverse personnel action.

Determining reprisal
Although proving reprisal can be complex, it starts with three simple questions:

1) Did the employee make a Protected Disclosure?
2) Was an adverse personnel action taken after the Protected Disclosure?
3) Was the Protected Disclosure a contributing factor in the decision to take the personnel action? This is often established by determining if the official taking personnel action had knowledge of the Protected Disclosure and if the official subsequently took an improper personnel action.

If the answer is yes to *all three* questions, there is sufficient evidence to justify a reprisal investigation.

Determining reprisal *(continued)*
An IG investigator will see if the supervisor would have taken the same adverse action absent the employee blowing the whistle. The investigator will review all the evidence and determine if the reprisal claim has merit.

When supervisors follow the proper policies and procedures, document their decision making process, and treat employees with fairness, any adverse actions they take for appropriate reasons will likely be found as legitimate rather than reprisal. However, supervisors who fail to follow agency regulations and don't accurately and thoroughly document their employees' performance or non-whistleblowing related conduct will lack the evidence they need to clear themselves and the agency of reprisal allegations.

Knowledge: Supervisors or employees with authority over personnel actions must have knowledge of the Protected Disclosure. Whether the supervisor had knowledge that the employee reported wrongdoing is essential to proving reprisal. A supervisor can have knowledge in two ways:

- **Direct.** Evidence that shows the official *directly knows* the employee made a disclosure. For example, the employee included the official on an email to the IC Hotline.
- **Imputed** (also called *Constructive*). Think of this as "unwitting inheritance and implementation." For example, a departing supervisor left his successor an adverse action to implement against an employee. He did not to tell his successor his recommendation for the adverse action was unfounded or that the employee made a protected disclosure. The new supervisor fails to verify the departing supervisor's claims and implements the adverse action, unwittingly (constructively) reprising against the employee.

Adverse Personnel Action: The individual must have suffered an adverse personnel action. Adverse personnel actions can be any action affecting pay or benefits or significant changes in working conditions.

So, am I protected from the adverse personnel action?
Imagine we've determined the supervisor has knowledge of the employee's disclosure and took an adverse personnel action. However, just as every workplace communication is not a protected disclosure, not every adverse action a supervisor takes is a prohibited reprisal. Whistleblowing laws protect legitimate adverse personnel actions if the agency demonstrates that it would have taken the same action in the absence of a Protected Disclosure.

Other Reprisal Considerations:

- Only the supervisor's motivation to reprise is considered; not the employee's motive for blowing the whistle.
- Employee or applicant protection applies where the employer mistakes a person for the whistleblower.
- IC whistleblowers may seek the advice of any one of the oversight bodies identified in this training to further help you understand the rules addressing statutory reprisal before any potential adverse documentation reaches your personnel record.

KNOWLEDGE CHECK: QUESTION 3
Maria has been Dave's supervisor for five years and has consistently provided Dave with positive performance evaluations. This year, after Dave reported to Maria that he witnessed a coworker taking classified information home in violation of the agency's security protocols, Maria provided Dave with a negative performance evaluation.

Which of the following is true (select all that apply):
A. A negative performance evaluation is not an adverse personnel action.
B. Dave made a Protected Disclosure to Maria.
C. Maria had direct knowledge of Dave's Protected Disclosure.
D. Dave is automatically protected from the adverse personnel action.

> **Correct/Incorrect Feedback**: B and C are true. Negative performance evaluations may impact an employee's pay and benefits and, therefore, may be considered adverse personnel actions. Although Dave is protected from reprisal for his Protected Disclosure, he is not automatically protected against his supervisor taking legitimate adverse personnel actions.

LESSON 4: WHAT NEXT? REPRISAL REVIEW PROCESSES AND REMEDIES

Filing a Reprisal Complaint

Under PPD-19, each IC Element certified to the DNI that its personnel policies provide a process for employees to seek review of personnel actions that they allege as prohibited reprisal for a Protected Disclosure. The review process requires that the agency's IG conduct a review to determine whether a personnel action constitutes prohibited reprisal for a Protected Disclosure.

Employees should contact their agency's IG to answer questions about their agency's personnel policies, provide procedural guidance, and otherwise assist you in filing a complaint concerning alleged prohibited reprisal.

Agency IG Findings
Based on the investigation results, the agency IG 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. The agency head is not required to follow the IG's recommendations but is required to carefully consider the IG's findings and recommended actions.

Remedies Available
To the extent authorized by law, 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.

What if the agency IG does not find that there has been reprisal?
Under PPD-19, after exhausting the agency's review process, IC employees have an opportunity to request a review of their reprisal claim to an External Review Panel, which is chaired by the IC IG. The IC IG has the discretion to decline requests for appeal; however, if the request is accepted, the External Review Panel will complete the review within 180 days of accepting the appeal.

What should I expect from the External Review Panel?
If the External Review Panel determines that the individual was the subject of a prohibited reprisal for a Protected Disclosure, 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. The agency head shall carefully review the panel's recommendation and, within 90 days, inform the panel and the DNI of the action taken.

MODULE 4

SCOPE OF MODULE 4 –WHISTLEBLOWER BEST PRACTICES FOR MANAGERS AND SUPERVISORS
Module 4 of this training highlights best practices for managers and supervisors to promote whistleblowing as a critical component of Federal employment. This module applies only to Executive branch managers and supervisors, but may be useful to all Executive branch employees and contractors.

LESSON 1: REFRESHER

Recap of Whistleblower Training
In this training, we learned the following:

- What is and what is not whistleblowing
- How to make a Protected Disclosure
- Protections against reprisal under Presidential Policy Directive-19 (PPD-19) and, for the IC, the National Security Act
- How allegations of prohibited reprisal are established
- Review processes and remedies for prohibited reprisal

Common Sense Advice for Supervisors
To the furthest extent possible, PPD-19 adopts general Federal employee standards protecting whistleblowers. This requires agencies to establish that they would have acted regardless of knowing the employee made a protected disclosure. Supervisors must be familiar with whistleblower protections and processes.

LESSON 2: TRAITS OF EFFECTIVE SUPERVISORS

Best Practices for Supervisors
Supervisors are most effective when they:

- Foster an open work environment that empowers employees to report wrongdoing.
- Closely adhere to merit-based performance management.
- Treat all employees fairly and consistently.
- Consistently and accurately document and routinely discuss their employee's performance.
- Are mindful that negligent or imprudent actions may lead to the appearance of wrongdoing.
- Seek advice from OGC when they have questions.

LESSON 3: BEST PRACTICES FOR SUPERVISORS

What should I do if an employee comes to me with an allegation of wrongdoing?
If someone on your staff wants to make a Protected Disclosure, alleges reprisal by another individual, or otherwise asks for advice concerning an allegation of wrongdoing:

- Ask questions – get as many details as you can from the employee.
- Encourage the employee to write up his/her concerns and include all relevant information, such as the facts leading to the employee's belief that some wrongdoing occurred.
- Document your conversation with the employee – make a note of the date/time of the conversation, details of what both you and the employee said, and what advice you gave the employee.
- Encourage the employee to contact your agency's IG so that it can be reviewed.
- If you think the employee's allegation has merit or if you are unsure of the allegation's merits, consult with and report it to your supervisor or other appropriate agency official (OGC, EEO, CLPT, IG, security, etc.), assuming they're not the subject of the allegations.
- Be discreet – do not bring it up in front of other employees.

Remember – you have a responsibility as a supervisor to receive whistleblower complaints from your employees. If you have questions, seek assistance from your agency's OGC.

What should supervisors not do?
As a supervisor, you are responsible for receiving complaints of wrongdoing. However, you are not responsible for investigating the allegations yourself – leave that to the investigators. You do not want to inadvertently destroy evidence, disclose the identity of an anonymous whistleblower, tip off any accused individual, or engage in any activity that could later be viewed as retaliatory toward the whistleblower. Seek expert advice from OGC and continue to exercise your normal duties as a supervisor.

Other actions supervisors must not do include:

- Dismiss the allegation out of hand or without consideration of the merits.

- Tell the employee to ignore the alleged wrongdoing and continue with his/her work.
- Confront the accused individual.
- Disclose the allegation to unauthorized individuals.
- Destroy any documentation concerning the allegation.

KNOWLEDGE CHECK: QUESTION 1

Steven observes Megan print a large stack of classified documents at the end of the day. Curious, Steven follows Megan back to her office and watches as she places the documents in her purse before she leaves the office. Steven reports his observations to his supervisor.

Which of the following would be considered appropriate responses from the supervisor (select all that apply):

A. The supervisor asks Steven to write down everything he observed.
B. The supervisor tells Steven that Megan was probably just printing out some personal documents.
C. The supervisor contacts security personnel.
D. The supervisor waits until the next day and confronts Megan.

> **Correct/Incorrect Feedback**: A and C are correct. Supervisors should not dismiss allegations out of hand or attempt to confront the accused.

LESSON 4: BEST PRACTICES FOR PERSONNEL TAKING, RECOMMENDING, OR APPROVING ACTIONS AFFECTING AN EMPLOYEE'S ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION

Importance of Protecting Classified Information

National security requires the protection of classified information. The unauthorized disclosure of classified information can cause irreparable harm to the national security and loss of human life. It is essential that we consistently practice and comply with security policies to appropriately protect classified information, while also providing fair and equitable treatment to those employees and contractors upon whom we rely to protect our classified information.

What is Eligibility for Access to Classified Information?

Eligibility for Access to Classified Information refers to the initial determination allowing an employee access to classified information, in accordance with Executive Order (EO) 12968 and EO 10865, and to an employee's continued access to classified information under such orders.

Eligibility Determinations

Under EO 12968, eligibility for access to classified information is determined through an initial investigation and periodic reinvestigations that assess an employee's:

- Loyalty to the United States;
- Strength of character, including trustworthiness, honesty, reliability, discretion, and sound judgment;
- Freedom from conflicting allegiances and potential for coercion; and
- Willingness and ability to abide by regulations governing the use, handling, and protection of classified information.

What actions are prohibited under PPD-19?

PPD-19 prohibits, as reprisal for Protected Disclosures, any actions affecting an employee's or contractor's eligibility for access to classified information. These actions may include recommendations or referrals taken by a supervisor or other responsible management official that impact the individual's security clearance or otherwise would affect their eligibility for access to classified information.

Considerations for Supervisors

Supervisors need to remain vigilant in detecting illegality, while also ensuring that their employees are encouraged to report wrongdoing, even if the allegations concern classified information. If an employee comes to you with a report of wrongdoing, remember that the employee is fulfilling his/her reporting obligation and performing a service to the agency and the public by coming forward with such information so that it can be examined and any necessary corrective action taken. In most agencies, you have an obligation as a supervisor to receive such Protected Disclosures.

If you provide negative information concerning an employee or contractor to security clearance adjudicators or investigators, then be prepared to provide specific facts and documentation supporting the negative information. This is a good practice whether or not the employee or contractor has come to you with regard to suspected wrongdoing. Supervisors are prohibited from using a Protected Disclosure as the basis for taking actions affecting the employee's eligibility for access to classified information. Allegations that a supervisor engaged in reprisal will be reviewed and may result in action against the supervisor. Contact ODNI OGC if you have any questions.

If you have reason to believe that an employee leaked classified information to unauthorized individuals after making a Protected Disclosure, or if you reasonably believe that an employee otherwise engaged in wrongdoing, then contact your agency's IG or OGC. You have an obligation to report wrongdoing within your office.

KNOWLEDGE CHECK: QUESTION 2

Brian is promoted to a new directorate and is responsible for managing a classified program. After learning more about the program, Brian has concerns that the program is violating agency regulations. Brian reports his concerns to his supervisor.

Which of the following would be considered an appropriate response from the supervisor:
A. The supervisor encourages Brian to contact the agency IG or contacts the agency's IG himself in order to discuss Brian's allegations.
B. Given the classified nature of the program, the supervisor reports Brian to security personnel as a possible insider threat.
C. The supervisor requests that Brian undergo a new security clearance investigation.
D. The supervisor removes Brian from the classified program.

> **Correct/Incorrect Feedback**: A is correct. Supervisors should contact the agency IG or other authorized individuals after receiving a report of wrongdoing. Reporting wrongdoing is an employee's responsibility and should not be viewed as indicative of a possible insider threat. Supervisors must not take actions against the reporting employee that may affect eligibility to access classified information or would otherwise be retaliatory adverse personnel actions.

REVIEW AND CONCLUSION

Although whistleblowing laws continue to evolve to keep pace with the federal government's dynamic mission and workforce, the fundamentals remain constant:

1. We are required to report illegality, waste, fraud, or abuse;
2. There are specific processes for whistleblowing;
3. Employees and contractors are protected from retaliation when we adhere to these processes; and
4. Effective performance management plays a vital role in the whistleblowing mission.

Key Terms and Acronyms

Direct Knowledge: A supervisor has "actual knowledge" of an employee's protected disclosure when there is direct evidence of such knowledge.

CLPT: Office of Civil Liberties, Privacy, and Transparency

DNI: Director of National Intelligence

EO: In the context of this training, Executive Order - Orders issued by the President applicable across the Executive branch of the Federal government.

ERP: External Review Panel, chaired by the IC IG

Imputed *or* **Constructive Knowledge:** Sometimes known as "Unwitting inheritance." Knowledge that is attributed through circumstantial evidence, such as a supervisor's statement in the workplace that they suspect there is a whistleblower in the office.

IC IG: Intelligence Community Inspector General, formally recognized as the Office of the Inspector General of the Intelligence Community

ICD: Intelligence Community Directive, issued by the DNI to establish policy and provide direction to the IC.

IC W&SP: Intelligence Community Whistleblowing & Source Protection program. Created in 2013 as part of the Office of Intelligence Community Inspector General (IC IG), this program works to ensure that employees who want to report wrongdoing can do so anonymously and without reprisal.

IG: Inspector General

Agency IG or **Local IG:** The Office of the Inspector General attached to a specific department or agency, e.g. CIA OIG, DIA OIG

OGC: Office of General Counsel

Personnel Action: any other significant change in duties, responsibilities, or working conditions. Examples include a reassignment, demotion, suspension, termination, performance evaluation, or a decision concerning pay.

PPD: Presidential Policy Directive

POTUS: President of the United States

Protected Disclosure: Information that an employee or contractor reasonably believes evidences a violation of law, rule, or regulation; or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, that the employee or contractor provides to a person or entity authorized to receive such disclosure, including:

- A supervisor in the employee's or contractor's chain-of-command;
- DNI (or designee);
- Employing agency head (or designee);
- IC IG;
- Their agency IG;
- Congressional intelligence committee or member of a congressional intelligence committee consistent with specific reporting procedures [insert link to: https://www.dni.gov/index.php/about-this-site/contact-the-ig/how-to-file-a-whistleblower-complaint]; and

- Other officials designated to receive Protected Disclosures. Depending on the nature of the allegation, these designated officials may include other compliance offices, such as your agency's Equal Employment Office (EEO), Office of General Counsel (OGC), your Intelligence Oversight (IO) officer, or your agency's (or ODNI's) Office of Civil Liberties, Privacy, and Transparency (CLPT).

See PPD-19 for the full definition of a "Protected Disclosure."

Whistleblower: an employee or contractor who reports information through the Protected Disclosure process that they reasonably believe evidences a violation of law, rule, or regulation; or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

Resources

- 5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch [insert link to: **[insert link to: https://www.oge.gov/Web/oge.nsf/0/076ABBBFC3B026A785257F14006929A2/$FILE/SOC%20as%20of%2076%20FR%2038547.pdf]**
- Executive Order 12674, Principles of Ethical Conduct for Government Officers and Employees **[insert link to: https://www.oge.gov/Web/OGE.nsf/Executive%20Orders/FA480E559E89F43A85257E96006A90F0/$FILE/2cffba1932d54681af32485c48d855282.pdf?open]**
- Presidential Policy Directive 19, Protecting Whistleblowers with Access to Classified Information **[insert link to: https://www.whitehouse.gov/sites/default/files/image/ppd-19.pdf]**
- Intelligence Community Directive 120, Intelligence Community Whistleblower Protection **[insert link to https://www.dni.gov/files/documents/ICD/ICD%20120.pdf]**
- IC IG website **[insert link to: https://www.dni.gov/index.php/about-this-site/contact-the-ig]**
- [Agency IG] website **[insert link to Agency IG website]**
- Principles of Professional Ethics for the Intelligence Community **[insert link to: https://www.dni.gov/index.php/intelligence-community/principles-of-professional-ethics]**
- Congressional intelligence committee reporting procedures [insert link to: https://www.dni.gov/index.php/about-this-site/contact-the-ig/how-to-file-a-whistleblower-complaint]