**OVERVIEW OF THE FEDERAL SECTOR EEO PROCESS**

**Sterling L. DeRamus**

**Attorney at Law**

**2229 First Avenue North**

**Birmingham, Alabama 35203**

**(205) 504-0189**

**sderamus@deramuslaw.com**

[**www.deramuslaw.com**](http://www.deramuslaw.com)

There are four main stages to a federal sector EEO complaint: Informal Counseling, Formal Complaint, EEOC Hearing, and EEOC appeal. In this paper we will deal with all four procedural stages and provide appropriate tips for representing federal government employees in the EEO process. The primary source for this material is 29 C.F.R. § 1614, et seq.

1. **The Informal Complaint stage:** A Federal employee has 45 days within which to file a complaint of discrimination with their local EEO Counselor’s office. The EEO Counselor has a duty to counsel the employee about their complaint, to help them properly frame it, and to seek the basic facts and to seek a resolution. There are two main processes within this stage: Traditional Counseling and ADR (alternative dispute resolution). Traditional counseling lasts 30 days and there is a short report by the counselor concerning the matter. If the employee chooses ADR however, then the counseling period is extended an additional 60 days, or a total of 90 days.
2. **Formal Complaint stage:** Once the informal complaint stage is complete, the EEO Counselor will provide the employee with a Right to File letter. The employee then has 15 days from receipt to file a Formal Complaint. The formal complaint stage is more complicated, and requires the agency to complete a formal investigation within 180 days of the filing, unless it is amended, in which case, the deadline is extended 180 days beyond the last amendment, or 365 days from the original filing date. Upon completion of the Formal Investigation, the Agency should provide the Complainant with a Report of Investigation. This is more than a simple report though and should contain interviews, affidavits and extensive documentation. Typical ROI’s are in excess of 500 pages.
3. **EEO Hearing stage:** Once a ROI is received, or the 180-day deadline has passed, the complainant should file a request for a hearing with the EEOC office. The EEO hearing stage is much like a trial in federal court, but with an Administrative Judge (AJ) and no jury. The federal discovery rules are applied with only minor differences. Initially the judge will issue an “Acknowledgment and Order” covering the deadlines to complete discovery (typically 90 days), and also requiring that written discovery be commenced within 20 days of receipt. Depositions can be noticed at anytime before the close of discovery. Summary judgment is available as well to either party. If Summary Judgment is denied, then the claim will proceed to a full hearing in front of an AJ. An AJ has no subpoena powers outside of the federal government. Non-employees cannot be compelled to testify, but they can come voluntarily. Once a hearing is complete, the AJ will make a decision, and then the matter is returned to the Agency for a Final Agency Decision. Substantive Title VII law applies to AJ decisions, but they are not bound by Circuit Court opinions, only the U.S. Supreme Court and the EEOC appeals process, or the Office of Federal Operations in D.C.
4. **EEOC Appeal stage:** Once a Final Agency Decision (FAD) has been made, the Complainant can file an appeal within the EEOC to the Washington Headquarters to the Office of Federal Operations (OFO). Typically a Complainant has 30 days from receipt of the FAD to file their appeal, and then an additional 30 days after that to file a brief in support of the appeal. If the OFO makes a decision in the Complainant’s favor, the Agency has no right to file any further appeal to Federal Court. However they can ask for reconsideration within 30 days of a decision. Typically speaking the OFO will not however make a decision on damages, and instead order the Agency to do a supplemental investigation on the issue of damages. Their decision is however appealable to the OFO. OFO decisions are public records, and they are available on EEOC’s website as well as Lexis/Nexis. In Lexis they are under “Administrative Materials.”
5. Finally, a complainant can appeal to the local U.S. District Court at various stages of the process. Once the Formal Complaint is completed, an employee can request a FAD at anytime and then appeal to the U.S. District Court within 90 days, alternatively within 90 days of a decision by the EEOC’s OFO.
6. **Jurisdictional Points:** The EEO process is the primary avenue of relief for all agency actions except those that can be appealed to the Merit Systems Protection Board (*see,* below). Relief is available for employees who are subject to harassment, disciplinary matters up to 14 days or less suspension, failure to select/promote, and other matters. Generally, employees who do not have MSPB appeal rights can take more serious disciplinary actions such as terminations through the EEO process. Most conspicuously, this includes employees who have been terminated in a probationary status – i.e. with less than one year of Federal government employment. But this also includes Title 38 employees, which includes medical providers for the Department of Veterans Affairs, and Tennessee Valley Authority employees (as well as most other government corporations). However, Title 10 employees, i.e. all active military, do not have EEO procedural rights, nor do officers of the Uniformed Public Health Service (USUPHS) (Title 42 employees). National Guard Technicians are hybrid Title 10/Title 5 employees who are GS employees during the week and revert to military status on their regular drill weekend and for two weeks each year, or when otherwise activated. National Guard Techs acting in a civilian capacity do have EEO rights. Contractors are general excluded from EEO coverage, but can be considered employees in specific situations if the Agency exercises direct control over the contractor.

**OVERVIEW OF MERIT SYSTEMS PROTECTION BOARD PROCEDURES**

**Sterling L. DeRamus**

**Attorney at Law**

**2229 First Avenue North**

**Birmingham, Alabama 35203**

**(205) 504-0189**

**sderamus@deramuslaw.com**

[**www.deramuslaw.com**](http://www.deramuslaw.com)

 The Federal Government’s Merit Systems Protection Board (MSPB) has primary responsibility over the enforcement of disciplinary and whistleblower issues for federal employees. In this paper we will discuss the layout of the MSPB, its jurisdiction, and basic procedural steps, and along the way give a few practical pointers for individuals practicing in front of the MSPB.

 The MSPB consists of a Washington DC headquarters office and 8 regional offices as is illustrated below.



 The closest regional office for the Huntsville, Alabama area is the Atlanta Regional Office. However, practice in front of the MSPB is not limited to counsel in a particular state. Alabama attorneys can represent Federal employees in California without admission to the California bar. Most MSPB offices contain 4 – 5 Administrative Judges who hear cases.

 The full MSPB sits in Washington and hears appeals from the regional offices. Above the MSPB is the Federal Circuit Court of Appeals for the Federal Circuit in Washington DC which hears any appeals directly from the MSPB as any Federal Circuit Court would (i.e. full F.R.A.P. Rules apply). There is no appeal to the U.S. District Court on MSPB matters unless the case is a “mixed-case” involving a termination or greater than 14 day suspension that is also a violation of Title VII.

1. **Jurisdiction:** A full discussion of MSPB Jurisdiction is beyond the scope of this short paper, but a few general points are important.
	1. **Terminations:** This is the most common appeal to the MSPB. Federal employees who complete a probationary period of employment of one year or more, have a property interest in their continued employment and cannot be terminated without just cause, and given an opportunity to respond and a hearing in front of a neutral judge. That is the MSPB.
	2. **Suspensions greater than 14 days:** While rarely used, the MSPB, also has jurisdiction over disciplinary actions such as suspensions greater than 14 days. For suspensions of 14 days or less, there is no MSPB appeal right, but an EEO complaint is available if there is a violation of Title VII.
	3. **Mixed Cases**: Mixed cases are either terminations or suspensions of greater than 14 days where the Appellant (i.e. the federal employee) also claims a violation of Title VII. The procedures used are slightly different and there are several different options available.
	4. **Whistleblower:** Whistleblower retaliation is the second most appealed action to the MSPB.
	5. **VEOA:** Veterans Employment Opportunity Act, 5 U.S.C. §2108. If an employee or applicant was denied a position and is a 5 or 10 points Veterans Preference eligible candidate, but was selected over a non-Veteran, then the MSPB will hear an appeal that the Agency failed to properly apply their veteran’s preference in the selection process. Even TVA employees who have been denied a promotion and/or laid off in violation of the VEOA can appeal to the MSPB.
	6. **Who is not covered?** It is important to recognize which employees are not covered by the MSPB. In general, the MSPB applies to Title 5 employees (i.e. General Schedule employees) and certain other specific employees of federal agencies. Specifically absent are military officials (i.e. Title 10) (including National Guard Technicians), FBI agents, postal employees other than managers, or otherwise in the excepted service, USUPHS, certain government corporations (TVA, especially), and medical providers for the Department of Veterans Affairs – with the exception of psychologists. Additionally, CIA employees and certain employees of the Defense Intelligence Agency and National Security Agency have no MSPB appeal rights.
	7. **Exceptions to lack of coverage:** Certain veterans may be able claim jurisdiction in specific instances. For example, TVA employees who are Veterans who are terminated may be able to claim violations of the VEOA, or Veterans Re-employment Act. A much larger example includes whistleblowers who otherwise do not have MSPB jurisdiction. Thus for example, a VA Physician alleging termination due to filing a complaint of wrongdoing can appeal to the MSPB. MSPB also has jurisdiction over the Reductions In Force Act (RIF), 5 U.S.C. § 3502, 5 CFR Part 351, and as such, TVA employees who claim that the Agency mis-applied the RIF statute to their particular situation can file an appeal with the Board. In general, the big exceptions include Veterans and Whistleblowers but particular research is needed in both cases to determine their eligibility for an appeal to the MSPB.
2. **MSPB Basic Procedures:** The MSPB operates on a tight schedule, and ideally all claims must be decided within a 140 day time frame from the date of filing an appeal. Employees who file an appeal are known as Appellants. The board operates an electronic appeals filing system that can be easily accessed.
	1. **Time lines:** Employees generally have 30 days from the date of an adverse action to appeal the action to the Board. This may be tolled in certain situations, specifically if the Agency fails to notify an employee of their appeal rights (e.g., forced disability retirements), and other specific tolling issues. Once the Administrative Judge makes a preliminary decision, the employee has 30 days to appeal the decision to the full MSPB in Washington prior to it becoming final. Simultaneously with the appeal, the brief must be filed. A petition for review can be filed with the Federal Circuit Court of Appeals for the Federal Circuit in Washington, DC within 35 days of an adverse ruling from the full MSPB. Both an appellant and an Agency can file petitions for review. Thus it is essential to be a member of that Circuit Court’s bar.
	2. **Jurisdictional Brief**:In whistleblower appeals, the first step will be a jurisdictional brief to ensure that the appeal is not frivolous. Be aware that it may take several months for the Board to determine whether jurisdiction is warranted.
	3. **Acknowledgment and Order:** Once an appeal is filed, the Administrative Judge will issue an Acknowledgment and Order setting out discovery deadlines. The Order will require that the Agency submit its agency file on the employee within a short time. This should include all applicable documents on the employee, including his personnel file, and documents associated with the adverse action. Following receipt of that typical discovery is allowed including interrogatories, document requests and requests for admission.
	4. **Prehearing and Hearing:** Just as in Federal Court there will be a prehearing order requiring the parties to submit their documents and witness lists. However, unlike federal court, there is no Summary Judgment procedure available at the MSPB. At a hearing the initial burden of proof is on the Agency, not the employee. However, affirmative defenses are on the employee to prove. In some situations, the Administrative Judge may bifurcate the hearing to determine damages. However back pay calculations are not required as they will be done by the Agency’s Human Resources Office subject to appeal.
	5. **Special Procedures for Mixed Cases:** Mixed cases involve those where the employee asserts discrimination under Title VII as an affirmative defense and these can be handled very differently. The employee has two avenues, including a) an immediate filing of an MSPB appeal, or b) filing a standard EEO complaint, including an informal complaint and then a formal complaint with the Agency. The latter option is generally preferred because of the extensive free discovery that the employee gets through the formal investigative stage. The same EEO procedures apply initially, however, upon completion of the Agency’s formal investigation, the employee then appeals to the MSPB instead of the EEOC. After the conclusion of the MSPB hearing the employee has the right to appeal the decision to the appropriate Federal District Court instead of being limited to appeals through the Federal Circuit Court of Appeals for the Federal Circuit.
	6. **Special Procedures for Whistleblower Cases:** Prior to filing a whistleblower appeal with the MSPB, the employee must first file their complaint with the Office of Special Counsel (OSC) (<https://osc.gov/> ). Once OSC has made a determination, the employee will have 65 days to file an appeal with the MSPB.
3. **Substantive Employee Rights:** What follows is a short discussion of some of the rights and standards of Federal employees who do have MSPB appeal rights in both disciplinary actions and whistleblower actions.
	1. **Disciplinary Actions:** Employees of the Federal government cannot be disciplined without cause. Adverse actions taken against federal employees require specific procedures to be followed in specific situations before the imposition of discipline. In general, prior to the imposition of discipline such as a termination or suspension, there should first be an investigation, followed by a proposed action with sufficient time to respond (practice pointer: always ask for an extension!), and a senior deciding official who is generally separate from the recommending official. Any proposed discipline should be analyzed through what are known as the twelve *Douglas* factors. *Douglas v. VA,* 5 MSPB 313 (1981):
		1. The nature and seriousness of the offense, and its relation to the employee’s duties, position, and responsibilities, including whether the offense was intentional or technical or inadvertent, or was committed maliciously or for gain, or was frequently repeated;
		2. the employee’s job level and type of employment, including supervisory or fiduciary role, contacts with the public, and prominence of the position;
		3. the employee’s past disciplinary record;
		4. the employee’s past work record, including length of service, performance on the job, ability to get along with fellow workers, and dependability;
		5. the effect of the offense upon the employee’s ability to perform at a satisfactory level and its effect upon supervisors’ confidence in the employee’s work ability to perform assigned duties;
		6. consistency of the penalty with those imposed upon other employees for the same or similar offenses;
		7. consistency of the penalty with any applicable agency table of penalties;
		8. the notoriety of the offense or its impact upon the reputation of the agency;
		9. the clarity with which the employee was on notice of any rules that were violated in committing the offense, or had been warned about the conduct in question;
		10. the potential for the employee’s rehabilitation;
		11. mitigating circumstances surrounding the offense such as unusual job tensions, personality problems, mental impairment, harassment, or bad faith, malice or provocation on the part of others involved in the matter; and
		12. the adequacy and effectiveness of alternative sanctions to deter such conduct in the future by the employee or others.
	2. **Performance Issues:** If a federal employee is terminated for performance issues instead of misconduct, the employee must first be allowed to demonstrate that they can improve their performance. This is known as the Performance Improvement Plan or PIP. There is a large body of case law on what constitutes an adequate PIP, but in general a PIP must be detailed, specific, and reasonably achievable. The employee must have help available to them during the PIP process. Adequate time for improvement is also required.
	3. **Whistleblower Issues:** 5 U.S.C. §2302(b)(8) contains the substantive provisions of the Whistleblower Protection Enhancement Act of 2012. It’s best to replicate it in toto:

**(b)** Any employee who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority—

**. . .**

**(8)** take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment because of—

**(A)** any disclosure of information by an employee or applicant which the employee or applicant reasonably believes evidences—

**(i)**

any 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,

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

**(B)** any disclosure to the Special Counsel, or to the Inspector General of an agency or another employee designated by the head of the agency to receive such disclosures, of information which the employee or applicant reasonably believes evidences—

**(i)**

any violation (other than a violation of this section) 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;

There are several key points to understand about this statute. First, complaints cannot be about frivolous or trivial matters (e.g., the coffee was not good), but instead, the employee should identify the specific violation of a statute, the code of federal regulations, or agency internal rule (e.g. timekeeping). This is part of the initial jurisdictional brief and in that brief it is vital to demonstrate that the complaint was not over minor problems that generally affect the workplace. Saying my boss is mean is not good enough. Additionally, the MSPB will deny jurisdiction for EEO retaliation cases, despite the plain reading of the statute. Such claims need to be made through the standard EEO process. Damages for emotional distress are available without limitation – unlike the $300,000 cap on EEO damages. Employees who do not file complaints, but are harassed or retaliated against by supervisors who believe they have filed a complaint can make a claim under this provision. Employees who are whistleblowers must still perform. The filing of excessive frivolous whistleblower complaints can be grounds for discipline.

1. **Other important issues:** The two most important statutes to understand in representing federal employees are: 5 U.S.C. §2301 and 5 U.S.C. §2302. §2301 lays out the basic Merit Systems principles for all employees and supervisors to follow. §2302 explains specific prohibited personnel practices, e.g. prohibitions on political firing, nepotism, etc. In general any adverse action taken against an employee should be under this statute and §2302 can help to establish jurisdiction in front of the MSPB or EEOC.
2. **Further references:** All MSPB decisions are available on their website and on Lexis/Nexis under Administrative Materials. The best guide however is Peter Broida’s *A Guide to Merit Systems Protection Board Law and Practice*, published by Dewey Publishing. (http://deweypub.com/store/).However it is rather large, over 5,000 pages total in two volumes, and somewhat expensive at $650.

**SECURITY CLEARANCE APPEALS**

**Sterling L. DeRamus**

**Attorney at Law**

**2229 First Avenue North**

**Birmingham, Alabama 35203**

**(205) 504-0189**

**sderamus@deramuslaw.com**

[**www.deramuslaw.com**](http://www.deramuslaw.com)

 Finally, I would like to briefly discuss Security Clearance issues. Each Federal Agency has their own procedures, however the most involved are those from the Department of Defense and those will be discussed.

 All security clearances in all agencies are controlled by a Presidential Executive Order, 12968, signed by President Bill Clinton. It provides that all individuals who are deemed not to be allowed access to classified information be afforded the following procedures:

(1) provided as comprehensive and detailed a written explanation of the basis for that conclusion as the national security interests of the United States and other applicable law permit;

(2) provided within 30 days, upon request and to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (3 U.S.C. 552a), as applicable, any documents, records, and reports upon which a denial or revocation is based;

(3) informed of their right to be represented by counsel or other representative at their own expense; to request any documents, records, and reports as described in section 5.2(a)(2) upon which a denial or revocation is based; and to request the entire investigative file, as permitted by the national security and other applicable law, which, if requested, shall be promptly provided prior to the time set for a written reply;

(4) provided a reasonable opportunity to reply in writing to, and to request a review of, the determination;

(5) provided written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal;

(6) provided an opportunity to appeal in writing to a high level panel, appointed by the agency head, which shall be comprised of at least three members, two of whom shall be selected from outside the security field. Decisions of the panel shall be in writing, and final except as provided in subsection (b) of this section; and

(7) provided an opportunity to appear personally and to present relevant documents, materials, and information at some point in the process before an adjudicative or other authority, other than the investigating entity, as determined by the agency head. A written summary or recording of such appearance shall be made part of the applicant's or employee's security record, unless such appearance occurs in the presence of the appeals panel described in subsection (a)(6) of this section.

 However, the U.S. Supreme Court has ruled that individuals do NOT have a property interests in retaining access to classified information. *Navy v. Egan*, 484 U.S. 518 (1988). Nevertheless, most agencies have an internal procedure that allow for first a written appeal and subsequently a hearing of some type. DoD specifically has the “Defense Office of Hearings and Appeals” (DOHA) which handles all hearings on security clearances for civilian, military, and contractors (known as Industrial Security Clearances).

 **Procedures:** There are two basic steps in defending a security clearance. First is the written response. A security clearance applicant should receive a statement from the Agency outlining the specific reasons for the denial of the security clearance. This is called the Statement of Reasons. The applicant should be given 30 days to respond to the denial of the clearance at least (sometimes more can be requested). Often a clearance can be restored or granted on this reply so it is essential for early involvement of counsel, who can write a detailed legal brief in reply to the statement of reasons. If a written response fails to persuade the Agency, the applicant has an opportunity to request a full hearing in front of an Administrative Judge and to present testimony, evidence and witnesses on his behalf. There is no discovery however the Agency will provide full documentation to the applicant and his counsel, and that is the primary evidence used against the applicant. A decision by the Administrative Judge is reviewable by DOHA, and all DOHA decisions are published and available on Lexis/Nexis under Administrative Materials.

 **Substantive Law:** The primary substantive law for security clearances is known as the “Adjudicative Guidelines” which are part of the Executive Order. They are reproduced below. In general though the usual problems with applicants include excessive drug use, financial problems, past security violations, excessive misdemeanor convictions (felonies are an automatic bar), and documented psychological problems. As the Statement of Reasons will explain the specific adjudicative guidelines, this makes research on Lexis/Nexis relatively simple. Once under Administrative Materials, and DOHA decisions, simply put in the search block “Guideline H” (or whatever guideline is used) and all DOHA decisions under that guideline should then be readily available. It is important for counsel to address all mitigating factors addressed in the guidelines in their written response and at the hearing. The general legal standard however to use is the “whole person” concept, and that is that the Administrative Judge should look at the whole person and not merely their particular foibles that have gotten them in trouble. The full guidelines are reproduced below, but the headings are as follows:

1. Allegiance to the United States
2. Foreign Influence
3. Foreign Preference
4. Sexual Behavior
5. Personal Conduct
6. Financial Considerations
7. Alcohol Consumption
8. Drug Involvement
9. Psychological Conditions
10. Criminal Conduct
11. Handling Protected Information
12. Outside Activities
13. Use of Information Technology Systems

For further reading on each one see the State Department’s Website: <http://www.state.gov/m/ds/clearances/60321.htm>

**ADJUDICATIVE GUIDELINES**

**Guideline A:
Allegiance to the United States**

**3. The Concern***.*An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

**4. Conditions that could raise a security concern and may be disqualifying include:**

(a) involvement in, support of, training to commit, or advocacy of any act of sabotage, espionage, treason, terrorism, or sedition against the United States of America;

(b) association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

(c) association or sympathy with persons or organizations that advocate, threaten, or use force or violence, or use any other illegal or unconstitutional means, in an effort to:

(1) overthrow or influence the government of the United States or any state or local government;

(2) prevent Federal, state, or local government personnel from performing their official duties;

(3) gain retribution for perceived wrongs caused by the Federal, state, or local government;

(4) prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

**5. Conditions that could mitigate security concerns include:**

(a) the individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

(b) the individual's involvement was only with the lawful or humanitarian aspects of such an organization;

(c) involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest;

(d) the involvement or association with such activities occurred under such unusual circumstances, or so much times has elapsed, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or loyalty.

**Guideline B:
Foreign Influence**

**6. The Concern.** Foreign contacts and interests may be a security concern if the individual has divided loyalties or foreign financial interests, may be manipulated or induced to help a foreign person, group, organization, or government in a way that is not in U.S. interests, or is vulnerable to pressure or coercioon by any foreign interest. Adjudication under this Guideline can and should consider the identity of the foreign country in which the foreign contact or financial interest is located, including, but not limited to, such considerations as whether the foreign country is known to target United States citizens to obtain protected information and/or is associated with a risk of terrorism.

**7. Conditions that could raise a security concern and may be disqualifying include:**

(a) contact with a foreign family member, business or professional associate, friend, or other person who is a citizen of or resident in a foreign country if that contact creates a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion;

(b) connections to a foreign person, group, government, or country that create a potential conflict of interest between the individual's obligation to protect sensitive information or technology and the individual's desire to help a foreign person, group, or country by providing that information;

(c) counterintelligence information, that may be classified, indicates that the individual's access to protected information may involve unacceptable risk to national security;

(d) sharing living quarters with a person or persons, regardless of citizenship status, if that relationship creates a heightened risk of foreign inducement, manipulation, pressure, or coercion;

(e) a substantial business, financial, or property interest in a foreign country, or in any foreign-owned or foreign-operated business, which could subject the individual to heightened risk of foreign influence or exploitation;

(f) failure to report, when required, association with a foreign national;

(g) unauthorized association with a suspected or known agent, associate, or employee of a foreign intelligence service;

(h) indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, inducement, manipulation, pressure, or coercion;

(i) conduct, especially while traveling outside the U.S., which may make the individual vulnerable to exploitation, pressure, or coercion by a foreign person, group, government, or country.

**8. Conditions that could mitigate security concerns include:**

(a) the nature of the relationships with foreign persons, the country in which these persons are located, or the positions or activities of those persons in that country are such that it is unlikely the individual will be placed in a position of having to choose between the interests of a foreign individual, group, organization, or government and the interests of the U.S.;

(b) there is no conflict of interest, either because the individual's sense of loyalty or obligation to the foreign person, group, government, or country is so minimal, or the individual has such deep and longstanding relationships and loyalties in the U.S., that the individual can be expected to resolve any conflict of interest in favor of the U.S. interest;

(c) contact or communication with foreign citizens is so casual and infrequent that there is little likelihood that it could create a risk for foreign influence or exploitation;

(d) the foreign contacts and activities are on U.S. Government business or are approved by the cognizant security authority;

(e) the individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons, groups, or organizations from a foreign country;

(f) the value or routine nature of the foreign business, financial, or property interests is such that they are unlikely to result in a conflict and could not be used effectively to influence, manipulate, or pressure the individual.

**Guideline C:
Foreign Preference**

**9. The Concern.** When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

**10. Conditions that could raise a security concern and may be disqualifying include:**

(a) exercise of any right, privilege or obligation of foreign citizenship after becoming a U.S. citizen or through the foreign citizenship of a family member. This includes but is not limited to:

(1) possession of a current foreign passport;

(2) military service or a willingness to bear arms for a foreign country;

(3) accepting educational, medical,
retirement, social welfare, or other such benefits from a foreign country;

(4) residence in a foreign country to meet citizenship requirements;

(5) using foreign citizenship to protect financial or business interests in another country;

(6) seeking or holding political office in a foreign country;

(7) voting in a foreign election;

(b) action to acquire or obtain recognition of a foreign citizenship by an American citizen;

(c) performing or attempting to perform duties, or otherwise acting, so as to serve the interests of a foreign person, group, organization, or government in conflict with the national security interest;

(d) any statement or action that shows allegiance to a country other than the United States: for example, declaration of intent to renounce United States citizenship; renunciation of United States citizenship.

**11. Conditions that could mitigate security concerns include:**

(a) dual citizenship is based solely on parents' citizenship or birth in a foreign country;

(b) the individual has expressed a willingness to renounce dual citizenship;

(c) exercise of the rights, privileges, or obligations of foreign citizenship occurred before the individual became a U.S. citizen or when the individual was a minor;

(d) use of a foreign passport is approved by the cognizant security authority;

(e) the passport has been destroyed, surrendered to the cognizant security authority, or otherwise invalidated;

(f) the vote in a foreign election was encouraged by the United States Government.

**Guideline D:
Sexual Behavior**

**12. The Concern.** Sexual behavior that involves a criminal offense, indicates a personality or emotional disorder, reflects lack of judgment or discretion, or which may subject the individual to undue influence or coercion, exploitation, or duress can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. No adverse inference concerning the standards in the Guideline may be raised solely on the basis of the sexual orientation of the individual.

**13. Conditions that could raise a security concern and may be disqualifying include:**

(a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

(b) a pattern of compulsive, self-destructive, or high-risk sexual behavior that the person is unable to stop or that may be symptomatic of a personality disorder;

(c) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress;

(d) sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

**14. Conditions that could mitigate security concerns include:**

(a) the behavior occurred prior to or during adolescence and there is no evidence of subsequent conduct of a similar nature;

(b) the sexual behavior happened so long ago, so infrequently, or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(c) the behavior no longer serves as a basis for coercion, exploitation, or duress;

(d) the sexual behavior is strictly private, consensual, and discreet.

**Guideline E:
Personal Conduct**

**15. The Concern.** Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

(a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, and cooperation with medical or psychological evaluation;

(b) refusal to provide full, frank and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

**16. Conditions that could raise a security concern and may be disqualifying also include:**

(a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative;

(c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information;

(d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of:

(1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information;

(2) disruptive, violent, or other inappropriate behavior in the workplace;

(3) a pattern of dishonesty or rule violations;

(4) evidence of significant misuse of Government or other employer's time or resources;

(e) personal conduct or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group;

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment;

(g) association with persons involved in criminal activity.

**17. Conditions that could mitigate security concerns include:**

(a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;

(b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;

(c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur;

(e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress;

(f) association with persons involved in criminal activities has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

**Guideline F:
Financial Considerations**

**18. The Concern.**Failure or inability to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Compulsive gambling is a concern as it may lead to financial crimes including espionage. Affluence that cannot be explained by known sources of income is also a security concern. It may indicate proceeds from financially profitable criminal acts.

**19. Conditions that could raise a security concern and may be disqualifying include:**

(a) inability or unwillingness to satisfy debts;

(b) indebtedness caused by frivolous or irresponsible spending and the absence of any evidence of willingness or intent to pay the debt or establish a realistic plan to pay the debt.

(c) a history of not meeting financial obligations;

(d) deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;

(e) consistent spending beyond one's means, which may be indicated by excessive indebtedness, significant negative cash flow, high debt-to-income ratio, and/or other financial analysis;

(f) financial problems that are linked to drug abuse, alcoholism, gambling problems, or other issues of security concern.

(g) failure to file annual Federal, state, or local income tax returns as required or the fraudulent filing of the same;

(h) unexplained affluence, as shown by a lifestyle or standard of living, increase in net worth, or money transfers that cannot be explained by subject's known legal sources of income;

(i) compulsive or addictive gambling as indicated by an unsuccessful attempt to stop gambling, "chasing losses" (i.e. increasing the bets or returning another day in an effort to get even), concealment of gambling losses, borrowing money to fund gambling or pay gambling debts, family conflict or other problems caused by gambling.

**20. Conditions that could mitigate security concerns include:**

(a) the behavior happened so long ago, was so infrequent, or occurred under such circumstances that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) the conditions that resulted in the financial problem were largely beyond the person's control (e.g. loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation), and the individual acted responsibly under the circumstances;

(c) the person has received or is receiving counseling for the problem and/or there are clear indications that the problem is being resolved or is under control;

(d) the individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts;

(e) the individual has a reasonable basis to dispute the legitimacy of the past-due debt which is the cause of the problem and provides documented proof to substantiate the basis of the dispute or provides evidence of actions to resolve the issue;

(f) the affluence resulted from a legal source of income.

**Guideline G:
Alcohol Consumption**

**21. The Concern.** Excessive alcohol consumption often leads to the exercise of questionable judgment or the failure to control impulses, and can raise questions about an individual's reliability and trustworthiness.

**22. Conditions that could raise a security concern and may be disqualifying include:**

(a) alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, disturbing the peace, or other incidents of concern, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(b) alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(c) habitual or binge consumption of alcohol to the point of impaired judgment, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(d) diagnosis by a duly qualified medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;

(e) evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;

(f) relapse after diagnosis of alcohol abuse or dependence and completion of an alcohol rehabilitation program;

(g) failure to follow any court order regarding alcohol education, evaluation, treatment, or abstinence.

**23. Conditions that could mitigate security concerns include:**

(a) so much time has passed, or the behavior was so infrequent, or it happened under such unusual circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) the individual acknowledges his or her alcoholism or issues of alcohol abuse, provides evidence of actions taken to overcome this problem, and has established a pattern of abstinence (if alcohol dependent) or responsible use (if an alcohol abuser);

(c) the individual is a current employee who is participating in a counseling or treatment program, has no history of previous treatment and relapse, and is making satisfactory progress;

(d) the individual has successfully completed inpatient or outpatient counseling or rehabilitation along with any required aftercare, has demonstrated a clear and established pattern of modified consumption or abstinence in accordance with treatment recommendations, such as participation in meetings of Alcoholics Anonymous or a similar organization and has received a favorable prognosis by a duly qualified medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

**Guideline H:
Drug Involvement**

**24. The Concern.** Use of an illegal drug or misuse of a prescription drug can raise questions about an individual's reliability and trustworthiness, both because it may impair judgment and because it raises questions about a person's ability or willingness to comply with laws, rules, and regulations.

(a) Drugs are defined as mood and behavior altering substances, and include:

(1) Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens), and (2) inhalants and other similar substances;

(b) drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

**25. Conditions that could raise a security concern and may be disqualifying include:**

(a) Any drug abuse (see above definition);

(b) testing positive for illegal drug use;

(c) illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution; or possession of drug paraphernalia;

(d) diagnosis by a duly qualified medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

(e) evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

(f) failure to successfully complete a drug treatment program prescribed by a duly qualified medical professional;

(g) any illegal drug use after being granted a security clearance;

(h) expressed intent to continue illegal drug use, or failure to clearly and convincingly commit to discontinue drug use.

**26. Conditions that could mitigate security concerns include:**

(a) the behavior happened so long ago, was so infrequent, or happened under such circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) a demonstrated intent not to abuse any drugs in the future, such as:

(1) dissociation from drug-using associates and contacts;

(2) changing or avoiding the environment where drugs were used;

(3) an appropriate period of abstinence;

(4) a signed statement of intent with automatic revocation of clearance for any violation;

(c) abuse of prescription drugs was after a severe or prolonged illness during which these drugs were prescribed, and abuse has since ended;

(d) satisfactory completion of a prescribed drug treatment program, including but not limited to rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a duly qualified medical professional.

**Guideline I:
Psychological Conditions**

**27. The Concern.** Certain emotional, mental, and personality conditions can impair judgment, reliability, or trustworthiness. A formal diagnosis of a disorder is not required for there to be a concern under this guideline. A duly qualified mental health professional (e.g., clinical psychologist or psychiatrist) employed by, or acceptable to and approved by the U.S. Government, should be consulted when evaluating potentially disqualifying and mitigating information under this guideline. No negative inference concerning the standards in this Guideline may be raised solely on the basis of seeking mental health counseling.

**28. Conditions that could raise a security concern and may be disqualifying include:**

(a) behavior that casts doubt on an individual's judgment, reliability, or trustworthiness that is not covered under any other guideline, including but not limited to emotionally unstable, irresponsible, dysfunctional, violent, paranoid, or bizarre behavior;

(b) an opinion by a duly qualified mental health professional that the individual has a condition not covered under any other guideline that may impair judgment, reliability, or trustworthiness;

(c) the individual has failed to follow treatment advice related to a diagnosed emotional, mental, or personality condition, e.g. failure to take prescribed medication.

**29. Conditions that could mitigate security concerns include:**

(a) the identified condition is readily controllable with treatment, and the individual has demonstrated ongoing and consistent compliance with the treatment plan;

(b) the individual has voluntarily entered a counseling or treatment program for a condition that is amenable to treatment, and the individual is currently receiving counseling or treatment with a favorable prognosis by a duly qualified mental health professional;

(c) recent opinion by a duly qualified mental health professional employed by, or acceptable to and approved by the U.S. Government that an individual's previous condition is under control or in remission, and has a low probability of recurrence or exacerbation;

(d) the past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual no longer shows indications of emotional instability;

(e) there is no indication of a current problem.

**Guideline J:
Criminal Conduct**

**30. The Concern.** Criminal activity creates doubt about a person's judgment, reliability and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules and regulations.

**31. Conditions that could raise a security concern and may be disqualifying include:**

(a) a single serious crime or multiple lesser offenses;

(b) discharge or dismissal from the Armed Forces under dishonorable conditions;

(c) allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted;

(d) individual is currently on parole or probation;

(e) violation of parole or probation, or failure to complete a court-mandated rehabilitation program.

**32. Conditions that could mitigate security concerns include:**

(a) so much time has elapsed since the criminal behavior happened, or it happened under such unusual circumstances that it is unlikely to recur or does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) the person was pressured or coerced into committing the act and those pressures are no longer present in the person's life;

(c) evidence that the person did not commit the offense;

(d) there is evidence of successful rehabilitation; including but not limited to the passage of time without recurrence of criminal activity, remorse or restitution, job training or higher education, good employment record, or constructive community involvement.

**Guideline K:
Handling Protected Information**

**33. The Concern.**Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

**34. Conditions that could raise a security concern and may be disqualifying include:**

(a) deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences;

(b) collecting or storing classified or other protected information in any unauthorized location;

(c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment;

(d) inappropriate efforts to obtain or view classified or other protected information outside one's need to know;

(e) copying classified or other protected information in a manner designed to conceal or remove classification or other document control markings;

(f) viewing or downloading information from a secure system when the information is beyond the individual's need to know;

(g) any failure to comply with rules for the protection of classified or other sensitive information;

(h) negligence or lax security habits that persist despite counseling by management;

(i) failure to comply with rules or regulations that results in damage to the National Security, regardless of whether it was deliberate or negligent.

**35. Conditions that could mitigate security concerns include:**

(a) so much time has elapsed since the behavior, or it happened so infrequently or under such unusual circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;

(c) the security violations were due to improper or inadequate training.

**Guideline L:
Outside Activities**

**36. The Concern.** Involvement in certain types of outside employment or activities is of security concern if it poses a conflict of interest with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

**37. Conditions that could raise a security concern and may be disqualifying include:**

(a) any employment or service, whether compensated or volunteer, with:

(1) the government of a foreign country;

(2) any foreign national, organization, or other entity;

(3) a representative of any foreign interest;

(4) any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology;

(b) failure to report or fully disclose an outside activity when this is required.

**38. Conditions that could mitigate security concerns include:**

(a) evaluation of the outside employment or activity by the appropriate security or counterintelligence office indicates that it does not pose a conflict with an individual's security responsibilities or with the national security interests of the United States;

(b) the individual terminates the employment or discontinued the activity upon being notified that it was in conflict with his or her security responsibilities.

**Guideline M:
Use of Information Technology Systems**

**39. The Concern.** Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

**40. Conditions that could raise a security concern and may be disqualifying include:**

(a) illegal or unauthorized entry into any information technology system or component thereof;

(b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system;

(c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;

(d) downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system;

(e) unauthorized use of a government or other information technology system;

(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations.

(g) negligence or lax security habits in handling information technology that persist despite counseling by management;

(h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

**41. Conditions that could mitigate security concerns include:**

(a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur or does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available;

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.