



DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
1333 ISAAC HULL AVE SE
WASHINGTON NAVY YARD DC 20376-0001

IN REPLY REFER TO
NAVSEAINST 5527.1
Ser SEA 00P-012/043
16 Feb 2021

NAVSEA INSTRUCTION 5527.1

From: Commander, Naval Sea systems Command

Subj: NAVAL SEA SYSTEMS COMMAND SECURITY ACCOUNTABILITY
INSTRUCTION

Ref: (a) SECNAVINST 12752.1A
(b) Security Executive Agent Directive (SEAD) 4
(c) SECNAVINST 5510.37A
(d) NAVSEAINST 5510.21
(e) SECNAVINST 5510.30C
(f) DoD Directive 4500.54E of 28 December 2009
(g) Security Executive Agent Directive (SEAD) 3
(h) SECNAVINST 5510.36B
(i) DoDM 5200.01 Volume 1, DoD Information Security Program: Overview, Classification, and Declassification of 24 February 2012
(j) BUPERSINST 1610.10E
(k) NAVSEA M-5510.1
(l) DoDM 5200.01 Volume 3, DoD Information Security Program: Protection of Classified Information of 24 February 2012
(m) DoDM 5200.01 Volume 2, DoD Information Security Program: Marking of Classified Information of 24 February 2012
(n) DoD Instruction 5200.48 of 6 March 2020
(o) DoD Directive 5210.50 of 27 October 2014
(p) E.O. 13526
(q) E.O. 13556

Encl: (1) Appendix A, National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position
(2) Security Issues and Basic Accountability Process

1. Purpose. To establish accountability within Naval Sea Systems Command (NAVSEA) for security-related incidents and actions or circumstances representing a security concern; formalize reporting of adverse or questionable information and security incidents; and establish processes and procedures when security-related incidents are alleged, occur, or are reported. Processes, procedures, and accountability will follow the guidelines and procedures of references (a) through (q).

2. Policy. It is NAVSEA policy, per references (a) through (q), that military, civilian, and seated contractor personnel, be formally held accountable for security transgressions for

DISTRIBUTION STATEMENT A: Approved for public release. Distribution is unlimited.

questionable or unfavorable information about an individual that may impact the individual's eligibility for access to classified information or eligibility to occupy a sensitive position, regardless of where they occur. Reference (a) states that discipline must be used as a managerial tool to correct deficiencies in employee conduct and performance consistent with law and Department of Defense (DoD) policies, and provides a schedule of offenses and recommended remedies. Military, civilian, and seated contractor personnel will be formally held accountable:

a. For actions and adverse or questionable information representing national security concerns per reference (b) and actual or potential insider threat behavior per references (c) and (d) to include, but not limited to:

- (1) Singular or multiple security infractions.
- (2) Reported security violations.
- (3) Conduct, behavior, or actions delineated in enclosure (1).
- (4) Guilt in military non-judicial punishment or military criminal proceedings, as determined by authorized military convening authority or judicial authority.
- (5) Substantiated findings of culpability, or substantiation of conduct, behavior, or actions falling within enclosure (1), as determined by the Naval or NAVSEA Inspectors General, or NAVSEA's Command Review & Investigation Office personnel.
- (6) Positive urinalysis, or unlawful possession, use, sale, or purchase of prohibited controlled substances.
- (7) Culpability, guilt, behavior, or conduct leading to disciplinary action against civilian employees.
- (8) Misuse or abuse of information technology (IT) systems; or electronic spillage of classified or controlled unclassified information (CUI) onto systems not cleared for that level of information.
- (9) Failure to report official and personal foreign travel to prohibited countries or to countries in contravention of references (e), (f), and (g).

b. Through any application of the following accountability measures (accountability measures may be combined) including, but not limited to:

- (1) Verbal or written warning via counseling by a first- or second-line supervisor.
- (2) Informal management inquiry.

(3) Formal inquiry, investigation, or referral to the Navy Criminal Investigative Service (NCIS), per references (e) and (h).

(4) Performance or contribution assessments, or evaluations, per references (e), (i), (j), and (k).

(5) Incident reports in the Defense Information System for Security (DISS) per reference (e).

(6) Suspension of access to classified information and assignment to sensitive duties, CUI, physical access to facilities, or IT system access pending administrative, personnel, or adjudicative action.

(7) Reports on contractors to company's facility security officer (FSO).

(8) Civilian employee letters of requirement, caution, reprimand, suspension, or removal.

(9) Military letters or caution, censure, or reprimand, or administrative separation.

(10) Command recommendation of security clearance eligibility revocation to the DoD Consolidated Adjudication Facility (DoD CAF).

(11) Criminal prosecution.

3. Responsibilities. Per references (a) through (q):

a. All commanders and commanding officers, activity security managers, activity assistant security managers/coordinators, personnel and information security specialists, insider threat program managers, and information systems security managers must become familiar with and implement this policy and higher level guidance.

b. Subordinate commands must issue tailored command guidance per this instruction.

c. All military, civilian, and seated contractor personnel assigned or attached to the NAVSEA Enterprise are required to comply with this instruction.

d. The NAVSEA Enterprise will maintain and fully implement this security instruction.

4. Action

a. Commander, Naval Sea Systems Command (SEA 00) will:

(1) Direct, military, civilian, and seated contractor personnel, assigned or attached to NAVSEA HQ, be held accountable for paragraph 2a security transgressions or other transgressions that directly impact security clearance eligibility criteria, per paragraph 2b.

(2) Delegate security accountability oversight within the NAVSEA Enterprise to the NAVSEA HQ Director, Security Programs (SEA 00P).

b. SEA 00P/Activity Security Manager (ASM) and all functional counterparts within the NAVSEA Enterprise will:

(1) Monitor and oversee security accountability policy and activities of the NAVSEA Enterprise, to include enclosure (2) process.

(2) Facilitate coordination of security accountability matters within the NAVSEA Enterprise.

(3) Support the DoD continuous evaluation program requirements and investigate potential or actual insider threats, and take appropriate action, per references (c) and (e).

(4) Coordinate NAVSEA Enterprise security-related personnel actions with Total Force and Corporate Operations (SEA 10), Office of Counsel (SEA 00L), the supervisory chain of command, and, cognizant security authority for contractors, when applicable, to include access to information/facilities, security clearance eligibility, assignment to sensitive duties, suspension, or removal.

(5) Provide a record of NAVSEA Enterprise civilian personnel with completed security violation proceedings and findings of culpability to DoD Civilian Acquisition Workforce Personnel Demonstration (AcqDemo) Pay Pools or respective performance appraisal panel for their consideration in determining final contribution or performance assessment scores.

(6) Provide a record of NAVSEA Enterprise military personnel with completed security violation proceedings and findings of culpability to Director, Military Personnel (SEA 00M) for their consideration in determining ranking and fitness report or evaluation scores.

c. Director, Intelligence Operations Division (SEA 00G) and all functional counterparts within the NAVSEA Enterprise will:

(1) Hold military, civilian, and seated contractor personnel, assigned or attached to NAVSEA Enterprise, accountable for paragraph 2a security transgressions or other transgressions that directly impact eligibility for continued Sensitive Compartmented Information (SCI) and/or Special Access Program (SAP) access.

(2) Notify and coordinate with the ASM and the FSO for contractors, when SCI and/or SAP determinations, based upon derogatory reports, security transgressions, or other transgressions, directly impact a NAVSEA Enterprise member's security clearance eligibility or assignment to sensitive duties.

d. Deputy Commander, Cyber Engineering and Digital Transformation (SEA 03) and all functional counterparts within the NAVSEA Enterprise will:

(1) Hold military, civilian, and seated contractor personnel, assigned or attached to NAVSEA Enterprises, accountable for paragraph 2a security transgressions or other transgressions per reference (d) and paragraph 2b, and coordinate with the respective FSO for seated contractor personnel.

(2) Conduct and coordinate authorized network and systems audit and monitoring activities to detect and identify improper usage of IT devices within NAVSEA Enterprise.

(3) Report electronic spillages of classified information to the ASM per the timelines established in reference (1) and coordinate actions to mitigate impact of the data spill with Security. Per reference (1), the ASM is responsible to ensure policy requirements regarding an inquiry or investigation, notification, and damage assessment are met and security personnel have the overall lead for addressing such events.

(4) Report findings of improper IT device usage to the employee's supervisor and SEA 00P as soon as practicable for security accountability and insider threat assessment purposes.

e. SEA 00L or Command Judge Advocate (SEA 00J) will coordinate with all functional counterparts within the NAVSEA Enterprise to:

(1) Advise functional counterparts within the NAVSEA Enterprise to hold military, civilian, and seated contractor personnel, assigned or attached to NAVSEA Enterprises, accountable for paragraph 2a security transgressions or other transgressions per reference (d) and paragraph 2b, and coordinate with the respective FSO for seated contractor personnel.

(2) Report adjudicated findings and convictions, per paragraph 2a(4) and 2a(5), to SEA 00P as soon as practicable for security accountability and insider threat assessment purposes.

f. SEA 00M and all functional counterparts within the NAVSEA Enterprise will:

(1) Advise functional counterparts within the NAVSEA Enterprise to hold military, civilian, and seated contractor personnel, assigned or attached to SEA 00M, accountable for paragraph 2a security transgressions or other transgressions, per reference (d) and paragraph 2b, and coordinate with the respective FSO for seated contractor personnel.

(2) In coordination with SEA 00J, report allegations of Uniform Code of Military Justice (UCMJ) violations and convictions, per paragraph 2a(4), to SEA 00P as soon as practicable for security accountability and insider threat assessment purposes.

(3) Use the records of military personnel with completed security violation proceedings, provided by SEA 00P, as factors in determining ranking and fitness report or evaluation scores.

g. Director, Inspector General (SEA 00N) and all functional counterparts within the NAVSEA Enterprise will:

(1) Advise functional counterparts within the NAVSEA Enterprise to hold military, civilian, and seated contractor personnel, assigned or attached to SEA 00N, accountable for paragraph 2a security transgressions or other transgressions, per reference (d) and paragraph 2b, and coordinate with the respective FSO for seated contractor personnel.

(2) Report findings of culpability or substantiation, per paragraph 2a(5), to SEA 00P as soon as practicable for security accountability and insider threat assessment purposes.

h. Director, SEA 10 and all functional counterparts within the NAVSEA Enterprise will:

(1) Advise functional counterparts within the NAVSEA Enterprise to hold military, civilian, and seated contractor personnel, assigned or attached to SEA 10, accountable for paragraph 2a security transgressions or other transgressions per reference (d) and paragraph 2b, and coordinate with the respective FSO for seated contractor personnel.

(2) Ensure human resource personnel report personnel actions, per paragraphs 2a(3) through 2a(7), to SEA 00P as soon as practicable for security accountability and insider threat assessment purposes.

(3) Ensure the records of civilian personnel with completed security violation proceedings and findings of culpability, provided by SEA 00P are reported to AcqDemo Pay Pools or respective performance appraisal panels for their consideration in determining final contribution or performance assessment scores. Additionally, AcqDemo Pay Pools or respective performance appraisal panels will consider marking down supervisors, who have not been documenting derogatory security-related information on their employees, one level on their quality of performance rating.

i. Supervisors and all functional counterparts within the NAVSEA Enterprise will:

(1) Hold subordinate military, civilian, and seated contractor personnel, accountable for paragraph 2a security transgressions or other transgressions per reference (d) and paragraph 2b.

(2) For military and civilian personnel whose duties significantly involve the creating, handling, or management of classified information, reflect security as a critical and rated element in contribution or performance assessments, to include supervisor assessments regarding continued eligibility to access classified information, per references (e), (i), and (k). Transgressions of seated contractor personnel must be reported to the contracting officer representative and SEA 00P as soon as practicable.

(3) Document and report behavior that is considered disruptive, threatening, or falls into the category of an insider threat, per reference (c) and paragraph 2a(3), to SEA 00P as soon as practicable.

(4) Consider reference (a) Schedule of Offenses and Recommended Remedies, when holding civilian employees accountable.

j. Military, civilian, and seated contractor personnel assigned to or attached to NAVSEA commands, will:

(1) Report conduct or behavior that is considered disruptive, threatening, or falls into the category of insider threat, per reference (c) and paragraph 2a, to supervisors, SEA 00P, and NCIS as soon as practicable.

(2) Avoid negligence, complacency, conduct, and behaviors that compromise security or put security at risk.

5. Records Management

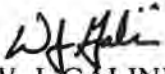
a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the Department of the Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page at <https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx>.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local records manager.

6. Review and effective date. Per OPNAVINST 5215.17A, SEA 00P will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, Department of Defense, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in

NAVSEAINST 5527.1
16 Feb 2021

effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.


W. J. GALINIS

Releasability and distribution:

This instruction is cleared for public release and is available electronically only, via the NAVSEA Intranet Web site located at
<https://navsea.navy.deps.mil/hq/Docs/Instructions/Forms/AllItems.aspx>

APPENDIX A**NATIONAL SECURITY ADJUDICATIVE GUIDELINES
FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION
OR ELIGIBILITY TO HOLD A SENSITIVE POSITION****I. Introduction.**

(a) The following National Security Adjudicative Guidelines ("guidelines") are established as the single common criteria for all U.S. Government civilian and military personnel, consultants, contractors, licensees, certificate holders or grantees and their employees, and other individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position, to include access to sensitive compartmented information, restricted data, and controlled or special access program information (hereafter referred to as "national security eligibility"). These guidelines shall be used by all Executive Branch Agencies when rendering any final national security eligibility determination.

(b) National security eligibility determinations take into account a person's stability, trustworthiness, reliability, discretion, character, honesty, and judgment. Individuals must be unquestionably loyal to the United States. No amount of oversight or security procedures can replace the self-discipline and integrity of an individual entrusted to protect the nation's secrets or occupying a sensitive position. When a person's life history shows evidence of unreliability or untrustworthiness, questions arise as to whether the individual can be relied upon and trusted to exercise the responsibility necessary for working in an environment where protecting the national security is paramount.

(c) The U.S. Government does not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in making a national security eligibility determination. No negative inference concerning eligibility under these guidelines may be raised solely on the basis of mental health counseling. No adverse action concerning these guidelines may be taken solely on the basis of polygraph examination technical calls in the absence of adjudicatively significant information.

(d) In accordance with EO 12968, as amended, eligibility for covered individuals shall be granted only when facts and circumstances indicate that eligibility is clearly consistent with the national security interests of the United States, and any doubt shall be resolved in favor of national security.

Enclosure (1)

2. The Adjudicative Process.

(a) The adjudicative process is an examination of a sufficient period and a careful weighing of a number of variables of an individual's life to make an affirmative determination that the individual is an acceptable security risk. This is known as the whole-person concept. All available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a national security eligibility determination.

(b) Each case must be judged on its own merits, and the final determination remains the responsibility of the authorized adjudicative agency. Any doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security.

(c) The ultimate determination of whether the granting or continuing of national security eligibility is clearly consistent with the interests of national security must be an overall common sense judgment based upon careful consideration of the following guidelines, each of which is to be evaluated in the context of the whole person.

- (1) GUIDELINE A: Allegiance to the United States
- (2) GUIDELINE B: Foreign Influence
- (3) GUIDELINE C: Foreign Preference
- (4) GUIDELINE D: Sexual Behavior
- (5) GUIDELINE E: Personal Conduct
- (6) GUIDELINE F: Financial Considerations
- (7) GUIDELINE G: Alcohol Consumption
- (8) GUIDELINE H: Drug Involvement and Substance Misuse
- (9) GUIDELINE I: Psychological Conditions
- (10) GUIDELINE J: Criminal Conduct
- (11) GUIDELINE K: Handling Protected Information
- (12) GUIDELINE L: Outside Activities
- (13) GUIDELINE M: Use of Information Technology

(d) In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

- (1) the nature, extent, and seriousness of the conduct;
- (2) the circumstances surrounding the conduct, to include knowledgeable participation;
- (3) the frequency and recency of the conduct;
- (4) the individual's age and maturity at the time of the conduct;
- (5) the extent to which participation is voluntary;
- (6) the presence or absence of rehabilitation and other permanent behavioral changes;
- (7) the motivation for the conduct;
- (8) the potential for pressure, coercion, exploitation, or duress; and
- (9) the likelihood of continuation or recurrence.

(c) Although adverse information concerning a single criterion may not be sufficient for an unfavorable eligibility determination, the individual may be found ineligible if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or unstable behavior. However, a single criterion may be sufficient to make an unfavorable eligibility determination even in the absence of a recent occurrence or a recurring pattern. Notwithstanding the whole-person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

(f) When information of security concern becomes known about an individual who is currently eligible for access to classified information or eligible to hold a sensitive position, the adjudicator should consider whether the individual:

- (1) voluntarily reported the information;
- (2) was truthful and complete in responding to questions;
- (3) sought assistance and followed professional guidance, where appropriate;
- (4) resolved or appears likely to favorably resolve the security concern;
- (5) has demonstrated positive changes in behavior; and
- (6) should have his or her national security eligibility suspended pending final adjudication of the information.

(g) If after evaluating information of security concern, the adjudicator decides the information is serious enough to warrant a recommendation of denial or revocation of the national security eligibility, but the specific risk to national security can be managed with appropriate mitigation measures, an adjudicator may recommend approval to grant initial or continued eligibility for access to classified information or to hold a sensitive position with an exception as defined in Appendix C.

(h) If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of denial or revocation of the national security eligibility, an adjudicator may recommend approval with a warning that future incidents of a similar nature or other incidents of adjudicative concern may result in revocation of national security eligibility.

(i) It must be noted that the adjudicative process is predicated upon individuals providing relevant information pertaining to their background and character for use in investigating and adjudicating their national security eligibility. Any incident of intentional material falsification or purposeful non-cooperation with security processing is of significant concern. Such conduct raises questions about an individual's judgment, reliability, and trustworthiness and may be predictive of their willingness or ability to protect the national security.

GUIDELINES**GUIDELINE A: ALLEGIANCE TO THE UNITED STATES**

3. *The Concern.* The willingness to safeguard classified or sensitive information is in doubt if there is any reason to suspect an individual's allegiance to the United States. There is no positive test for allegiance, but there are negative indicators. These include participation in or support for acts against the United States or placing the welfare or interests of another country above those of the United States. Finally, the failure to adhere to the laws of the United States may be relevant if the violation of law is harmful to stated U.S. interests. An individual who engages in acts against the United States or provides support or encouragement to those who do has already demonstrated willingness to compromise national security.

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;
- (b) association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts; and
- (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 U.S. Government 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; and
 - (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 humanitarian and permitted under U.S. law;
- (c) involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest; and

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

GUIDELINE B: FOREIGN INFLUENCE

6. *The Concern.* Foreign contacts and interests, including, but not limited to, business, financial, and property interests, are a national security concern if they result in divided allegiance. They may also be a national security concern if they create circumstances in which the individual may be manipulated or induced to help a foreign person, group, organization, or government in a way inconsistent with U.S. interests or otherwise made vulnerable to pressure or coercion by any foreign interest. Assessment of foreign contacts and interests should consider the country in which the foreign contact or interest is located, including, but not limited to, considerations such as whether it is known to target U.S. citizens to obtain classified or sensitive information or is associated with a risk of terrorism.

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

(a) contact, regardless of method, 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 classified or sensitive information or technology and the individual's desire to help a foreign person, group, or country by providing that information or technology;

(c) failure to report or fully disclose, when required, association with a foreign person, group, government, or country;

(d) counterintelligence information, whether classified or unclassified, that indicates the individual's access to classified information or eligibility for a sensitive position may involve unacceptable risk to national security;

(e) shared 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;

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

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

16 Feb 2021

(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; and

(i) conduct, especially while traveling or residing outside the U.S., that 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 United States;

(b) there is no conflict of interest, either because the individual's sense of loyalty or obligation to the foreign person, or allegiance to the group, government, or country is so minimal, or the individual has such deep and longstanding relationships and loyalties in the United States, 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 agency head or designee;

(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; and

(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 provide information or make decisions that are harmful to the interests of the United States. Foreign involvement raises concerns about an individual's judgment, reliability, and trustworthiness when it is in conflict with U.S. national interests or when the individual acts to conceal it. *By itself*, the fact that a U.S. citizen is also a citizen of another country is not disqualifying without an objective showing of such conflict or attempt at concealment. The same is true for a U.S. citizen's exercise of any right or privilege of foreign citizenship and any action to acquire or obtain recognition of a foreign citizenship.

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

16 Feb 2021

- (a) applying for and/or acquiring citizenship in any other country;
- (b) failure to report, or fully disclose when required, to an appropriate security official, the possession of a passport or identity card issued by any country other than the United States;
- (c) failure to use a U.S. passport when entering or exiting the U.S.;
- (d) participation in foreign activities, including but not limited to:
 - (1) assuming or attempting to assume any type of employment, position, or political office in a foreign government or military organization; and
 - (2) otherwise acting to serve the interests of a foreign person, group, organization, or government in any way that conflicts with U.S. national security interests;
- (e) using foreign citizenship to protect financial or business interests in another country in violation of U.S. law; and
- (f) an act of expatriation from the United States such as declaration of intent to renounce U.S. citizenship, whether through words or actions.

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

- (a) the foreign citizenship is not in conflict with U.S. national security interests;
- (b) dual citizenship is based solely on parental citizenship or birth in a foreign country, and there is no evidence of foreign preference;
- (c) the individual has expressed a willingness to renounce the foreign citizenship that is in conflict with U.S. national security interests;
- (d) the exercise of the rights, privileges, or obligations of foreign citizenship occurred before the individual became a U.S. citizen;
- (e) the exercise of the entitlements or benefits of foreign citizenship do not present a national security concern;
- (f) the foreign preference, if detected, involves a foreign country, entity, or association that poses a low national security risk;
- (g) civil employment or military service was authorized under U.S. law, or the employment or service was otherwise consented to as required by U.S. law; and
- (h) any potentially disqualifying activity took place after receiving the approval by the agency head or designee.

GUIDELINE D: SEXUAL BEHAVIOR

12. The Concern. Sexual behavior that involves a criminal offense; reflects a lack of judgment or discretion; or may subject the individual to undue influence of coercion, exploitation, or duress. These issues, together or individually, may raise questions about an individual's judgment, reliability, trustworthiness, and ability to protect classified or sensitive information. Sexual behavior includes conduct occurring in person or via audio, visual, electronic, or written transmission. No adverse inference concerning the standards in this 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 individual is unable to stop;
- (c) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress; and
- (d) sexual behavior of a public nature or that 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 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; and
- (e) the individual has successfully completed an appropriate program of treatment, or is currently enrolled in one, has demonstrated ongoing and consistent compliance with the treatment plan, and/or has received a favorable prognosis from a qualified mental health professional indicating the behavior is readily controllable with treatment.

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 or sensitive information. Of special interest is any failure to cooperate or provide truthful and candid answers during national security investigative or adjudicative processes. The following will normally result in an unfavorable national security eligibility determination, security clearance action, or cancellation of further processing for national security 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, cooperation with medical or psychological evaluation, or polygraph examination, if authorized and required; and

(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 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 national security eligibility or trustworthiness, or award fiduciary responsibilities;

(b) deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to an employer, investigator, security official, competent medical or mental health professional involved in making a recommendation relevant to a national security eligibility determination, 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 individual may not properly safeguard classified or sensitive 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 individual may not properly safeguard classified or sensitive 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 government protected information;
- (2) any disruptive, violent, or other inappropriate behavior;

- (3) a pattern of dishonesty or rule violations; and
 - (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 by a foreign intelligence entity or other individual or group. Such conduct includes:
- (1) engaging in activities which, if known, could affect the person's personal, professional, or community standing;
 - (2) while in another country, engaging in any activity that is illegal in that country;
 - (3) while in another country, engaging in any activity that, while legal there, is illegal in the United States;
- (f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment; and
- (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 advice of legal counsel or of a person with professional responsibilities for advising or instructing the individual specifically concerning security processes. 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 contributed to 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) the information was unsubstantiated or from a source of questionable reliability; and

(g) association with persons involved in criminal activities was unwitting, 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 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 or sensitive information. Financial distress can also be caused or exacerbated by, and thus can be a possible indicator of, other issues of personnel security concern such as excessive gambling, mental health conditions, substance misuse, or alcohol abuse or dependence. An individual who is financially overextended is at greater risk of having to engage in illegal or otherwise questionable acts to generate funds. Affluence that cannot be explained by known sources of income is also a security concern insofar as it may result from criminal activity, including espionage.

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

- (a) inability to satisfy debts;
- (b) unwillingness to satisfy debts regardless of the ability to do so;
- (c) a history of not meeting financial obligations;
- (d) deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, expense account fraud, mortgage fraud, filing deceptive loan statements and other intentional financial breaches of trust;
- (e) consistent spending beyond one's means or frivolous or irresponsible spending, which may be indicated by excessive indebtedness, significant negative cash flow, a history of late payments or of non-payment, or other negative financial indicators;
- (f) failure to file or fraudulently filing annual Federal, state, or local income tax returns or failure to pay annual Federal, state, or local income tax as required;
- (g) unexplained affluence, as shown by a lifestyle or standard of living, increase in net worth, or money transfers that are inconsistent with known legal sources of income;
- (h) borrowing money or engaging in significant financial transactions to fund gambling or pay gambling debts; and
- (i) concealing gambling losses, 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, a death, divorce or separation, clear victimization by predatory lending practices, or identity theft), and the individual acted responsibly under the circumstances;

(c) the individual has received or is receiving financial counseling for the problem from a legitimate and credible source, such as a non-profit credit counseling service, and there are clear indications that the problem is being resolved or is under control;

(d) the individual initiated and is adhering to 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; and

(g) the individual has made arrangements with the appropriate tax authority to file or pay the amount owed and is in compliance with those arrangements.

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 the frequency of the individual's alcohol use or whether the individual has been diagnosed with alcohol use disorder;

(b) alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, drinking on the job, or jeopardizing the welfare and safety of others, regardless of whether the individual is diagnosed with alcohol use disorder;

(c) habitual or binge consumption of alcohol to the point of impaired judgment, regardless of whether the individual is diagnosed with alcohol use disorder;

(d) diagnosis by a duly qualified medical or mental health professional (e.g., physician, clinical psychologist, psychiatrist, or licensed clinical social worker) of alcohol use disorder;

(e) the failure to follow treatment advice once diagnosed;

(f) alcohol consumption, which is not in accordance with treatment recommendations, after a diagnosis of alcohol use disorder; and

(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 judgment;

(b) the individual acknowledges his or her pattern of maladaptive alcohol use, provides evidence of actions taken to overcome this problem, and has demonstrated a clear and established pattern of modified consumption or abstinence in accordance with treatment recommendations;

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

(d) the individual has successfully completed a treatment program along with any required aftercare, and has demonstrated a clear and established pattern of modified consumption or abstinence in accordance with treatment recommendations.

GUIDELINE H: DRUG INVOLVEMENT¹ AND SUBSTANCE MISUSE

24. The Concern. The illegal use of controlled substances, to include the misuse of prescription and non-prescription drugs, and the use of other substances that cause physical or mental impairment or are used in a manner inconsistent with their intended purpose can raise questions about an individual's reliability and trustworthiness, both because such behavior may lead to physical or psychological impairment and because it raises questions about a person's ability or willingness to comply with laws, rules, and regulations. *Controlled substance* means any

¹ Reference Appendix B of this document regarding statutory requirements contained in Public Law 110-118 (Bond Amendment) applicable to this guideline.

"controlled substance" as defined in 21 U.S.C. 802. *Substance misuse* is the generic term adopted in this guideline to describe any of the behaviors listed above.

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

- (a) any substance misuse (see above definition);
- (b) testing positive for an illegal drug;
- (c) illegal possession of a controlled substance, including cultivation, processing, manufacture, purchase, sale, or distribution; or possession of drug paraphernalia;
- (d) diagnosis by a duly qualified medical or mental health professional (e.g., physician, clinical psychologist, psychiatrist, or licensed clinical social worker) of substance use disorder;
- (e) failure to successfully complete a drug treatment program prescribed by a duly qualified medical or mental health professional;
- (f) any illegal drug use while granted access to classified information or holding a sensitive position; and
- (g) expressed intent to continue drug involvement and substance misuse, or failure to clearly and convincingly commit to discontinue such misuse.

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) the individual acknowledges his or her drug involvement and substance misuse, provides evidence of actions taken to overcome this problem, and has established a pattern of abstinence, including, but not limited to:
 - (1) disassociation from drug-using associates and contacts;
 - (2) changing or avoiding the environment where drugs were used; and
 - (3) providing a signed statement of intent to abstain from all drug involvement and substance misuse, acknowledging that any future involvement or misuse is grounds for revocation of national security eligibility;
- (c) abuse of prescription drugs was after a severe or prolonged illness during which these drugs were prescribed, and abuse has since ended; and

(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 CONDITIONS²

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 and an opinion, including prognosis, should be sought. No negative inference concerning the standards in this guideline may be raised solely on the basis of 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, stability, reliability, or trustworthiness, not covered under any other guideline and that may indicate an emotional, mental, or personality condition, including, but not limited to, irresponsible, violent, self-harm, suicidal, paranoid, manipulative, impulsive, chronic lying, deceitful, exploitative, or bizarre behaviors;

(b) an opinion by a duly qualified mental health professional that the individual has a condition that may impair judgment, stability, reliability, or trustworthiness;

(c) voluntary or involuntary inpatient hospitalization;

(d) failure to follow a prescribed treatment plan related to a diagnosed psychological/psychiatric condition that may impair judgment, stability, reliability, or trustworthiness, including, but not limited to, failure to take prescribed medication or failure to attend required counseling sessions; and

(e) pathological gambling, the associated behaviors of which may include unsuccessful attempts to stop gambling; gambling for increasingly higher stakes, usually in an attempt to cover losses; concealing gambling losses; borrowing or stealing money to fund gambling or pay gambling debts; and family conflict resulting from gambling.

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;

²

Reference Appendix B of this document regarding statutory requirements contained in Public Law 110-118 (Bond Amendment) applicable to this guideline.

(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 psychological/psychiatric condition was temporary, 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 CONDUCT³

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 pattern of minor offenses, any one of which on its own would be unlikely to affect a national security eligibility decision, but which in combination cast doubt on the individual's judgment, reliability, or trustworthiness;

(b) evidence (including, but not limited to, a credible allegation, an admission, and matters of official record) of criminal conduct, regardless of whether the individual was formally charged, prosecuted, or convicted;

(c) individual is currently on parole or probation;

(d) violation or revocation of parole or probation, or failure to complete a court-mandated rehabilitation program; and

(e) discharge or dismissal from the Armed Forces for reasons less than "Honorable."

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 and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

³Reference Appendix B of this document regarding statutory requirements contained in Public Law 110-118 (Bond Amendment) applicable to this guideline.

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

(c) no reliable evidence to support that the individual committed the offense; and

(d) there is evidence of successful rehabilitation; including, but not limited to, the passage of time without recurrence of criminal activity, restitution, compliance with the terms of parole or probation, 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 handling protected information—which includes classified and other sensitive government information, and proprietary 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 protected information to unauthorized persons, including, but not limited to, personal or business contacts, the media, or persons present at seminars, meetings, or conferences;

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

(c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium;

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

(e) copying or modifying protected information in an unauthorized 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 sensitive information;

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

(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 has happened 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;
- (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 or unclear instructions; and
- (d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

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 or sensitive 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; and
- (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; and

(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; and

(b) the individual terminated 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

39. *The Concern.* Failure to comply 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 includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate these operations.

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

- (a) unauthorized entry into any information technology system;
- (b) unauthorized modification, destruction, or manipulation of, or denial of access to, an information technology system or any data in such a 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, sensitive, proprietary, or other protected information on or to any unauthorized information technology system;
- (e) unauthorized use of any information technology system;
- (f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations or when otherwise not authorized;
- (g) negligence or lax security practices in handling information technology that persists despite counseling by management; and
- (h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

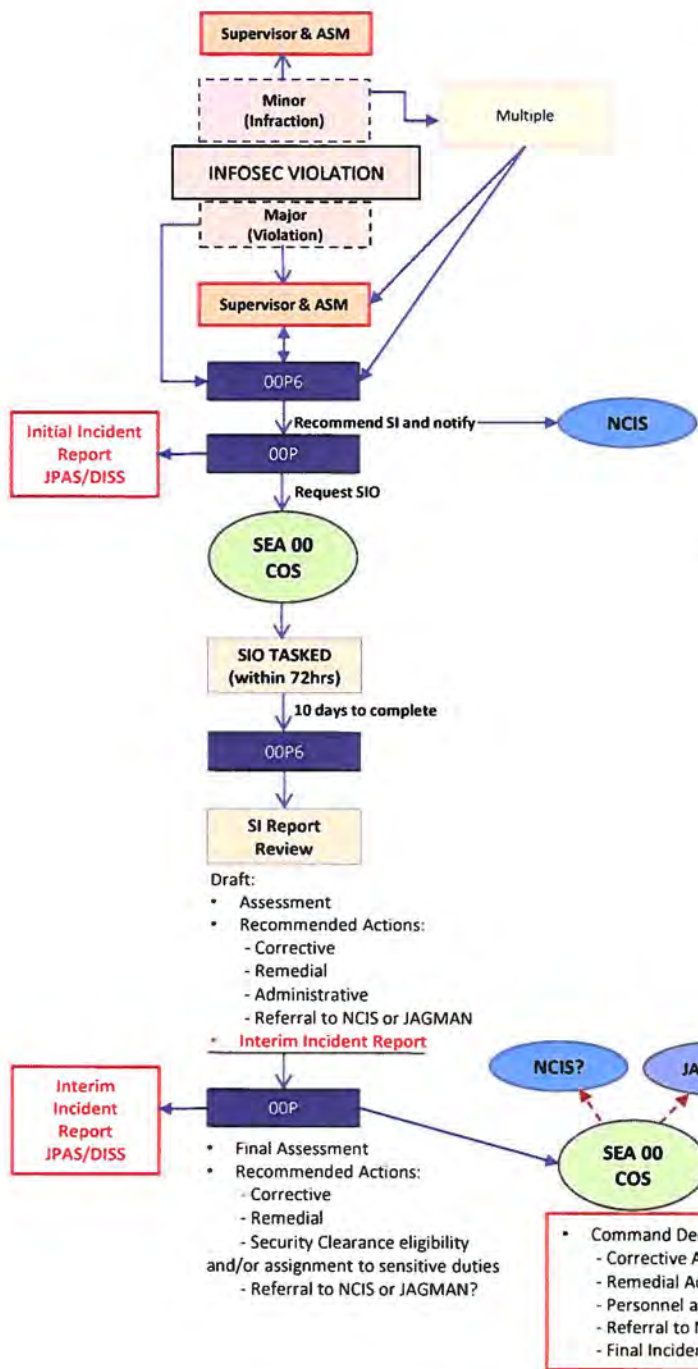
41. *Conditions that could mitigate security concerns include:*

- (a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;
- (b) the misuse was minor and done solely in the interest of organizational efficiency and effectiveness;

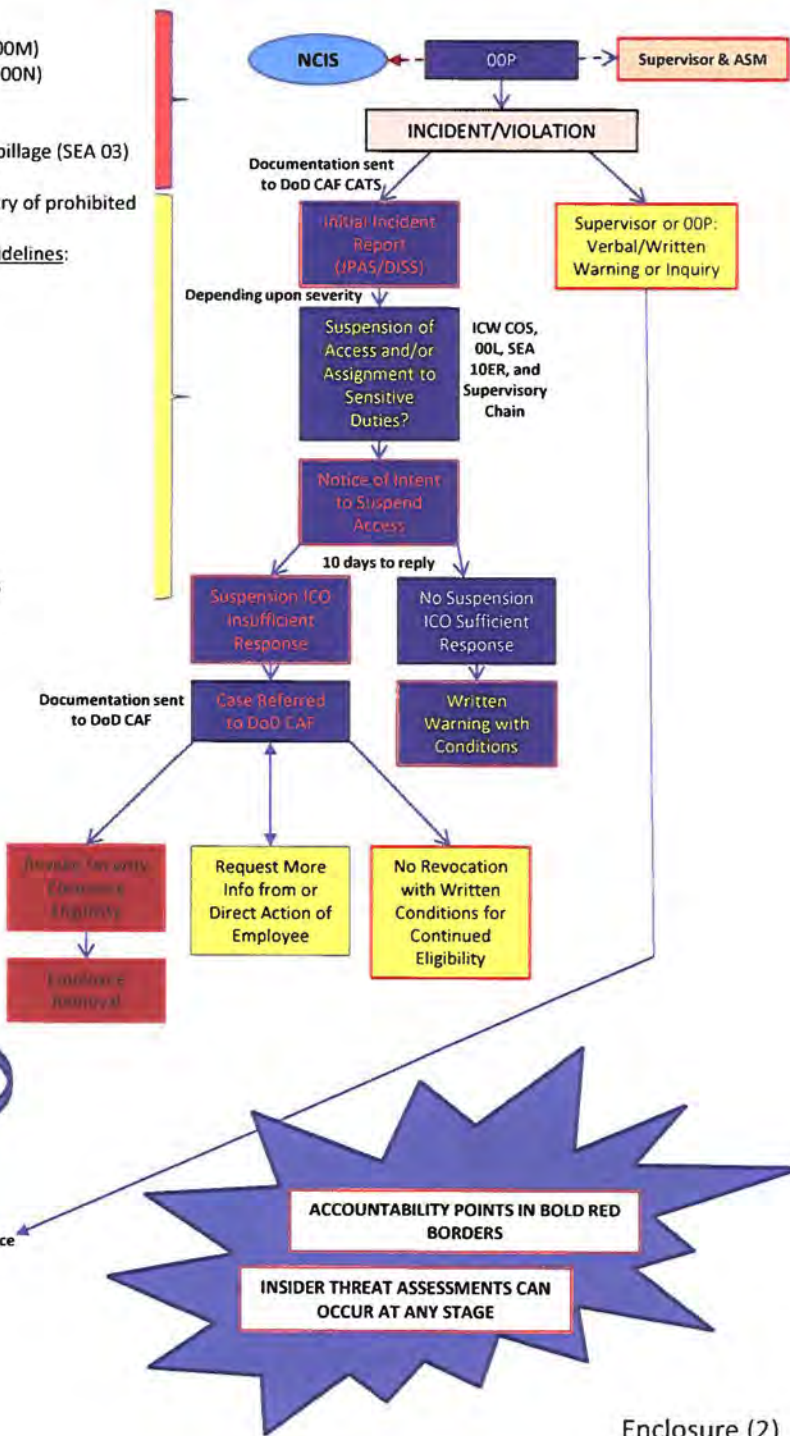
(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification to appropriate personnel; and

(d) the misuse was due to improper or inadequate training or unclear instructions.

SECURITY ISSUES AND BASIC ACCOUNTABILITY PROCESS



- Affirmed guilt in legal proceedings (SEA 00L)
- Affirmed guilt in military personnel discipline (SEA 00M)
- Culpability in Inspector General investigations (SEA 00N)
- Positive urinalysis results (SEA 00M and SEA 10)
- Employee disciplinary action (SEA 10 ER/EEO/HR)
- Confirmed Information Technology (IT) misuse or spillage (SEA 03)
- Confirmed Unreported Foreign Travel
- Security incidents (e.g., alleged assault, threats, entry of prohibited items, abandoned "Escort Required" visitors, etc.)
- Reported issues concerning the **13 Adjudicative Guidelines**:
 - Allegiance to the United States
 - Foreign Influence
 - Foreign Preference
 - Sexual Behavior
 - Personal Conduct
 - Financial Considerations
 - Alcohol Consumption
 - Drug Involvement
 - Psychological Conditions
 - Criminal Conduct
 - Handling Protected Information
 - Outside Activities
 - Use of Information Technology Systems
- To include violations occurring in other locations



- Command Decision to OOP:
 - Corrective Actions
 - Remedial Actions
 - Personnel action ICW SEA 00L, SEA 10 ER, and **Supervisor/COR**
 - Referral to NCIS or JAGMAN, or subject to above process?
 - Final Incident Report JPAS/DISS