



Security

Newsletter

September 2018

Adjudicative Guideline – Guideline K – HANDLING PROTECTED INFORMATION

By: DoDSecurity.Blogspot

This article is the eighth and final in a series of installments on the 13 Adjudicative Guidelines. As a reminder, these guidelines are being discussed as a means to simply provide guidance during the investigation process or, more importantly, to provide awareness for self-reporting requirements. If you are ever in doubt or worried about whether or not you should self-report, contact your Facility Security Officer or Program Manager.

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.

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;

Adjudicative Guideline – Guideline K (cont.)

- (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.

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.

Adjudicative Guideline – Guideline L – OUTSIDE ACTIVITIES

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.

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.

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.

Adjudicative Guideline – Guideline M – USE OF INFORMATION TECHNOLOGY

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.

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.

Adjudicative Guideline – Guideline M (Cont.)

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.

The Adjudicative Process - OVERVIEW

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.

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.

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.

Adjudicative Process – OVERVIEW (cont.)

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.

(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.

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.

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.

Adjudicative Process – OVERVIEW (cont).

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.

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.

Any Questions? Please contact us:

Holly Higgins /FSO: holly.higgins@wbsi.com or Charity Knutti /ALT FSO: charity@wbsi.com