NATIONAL CENTER FOR CREDIBILITY ASSESSMENT

PDD 504 METHODS I

TEST FOR ESPIONAGE AND SABOTAGE (TES)

Jan 2016

FOR OFFICIAL USE ONLY

This supersedes previous versions of this handout.

Table of Contents

1. Introduction

1.1. The Test for Espionage and Sabotage (TES) is a standardized psychophysiological detection of deception examination (polygraph) that is part of the counterintelligence (CI) screening process. The TES format provides a minimally intrusive means to assess the credibility of an examinee's answers to questions used in security pre-employment and periodic polygraph examinations, and to elicit information related to national security issues.

1.2. The following is a list of definitions used in this manual:

1.2.1. Significant Response (SR): Consistent physiological responses to the relevant questions in a multiple issue polygraph (MIP).

1.2.2. Deception Indicated (DI): Consistent physiological responses to the relevant questions in a single issue polygraph (SIP) using a probable lie comparison (PLC) question format.

1.2.3. No Significant Response (NSR): There is a lack of consistent physiological responses to the relevant questions in a MIP.

1.2.4. No Deception Indicated (NDI): There is lack of consistent physiological responses to the relevant questions in a SIP using a PLC format.

1.2.5. No Opinion (NO): Any examination that is not NSR/NDI or SR/DI.

1.2.6. Examination: The entire procedure, including all phases of a polygraph examination and, in the case of TES, both sub-tests, during a testing session.

1.2.7. Sub-test: The TES consists of two sub-tests. Each sub-test contains two relevant questions. Whichever sub-test is administered first those relevant questions must be resolved before the next sub-test can be administered.

1.2.8. Sequence: The order in which the questions will be asked.

1.2.9. Presentation: A single reading of a question.

1.2.10. Presentation score: The numerical evaluation for a specific relevant presentation.

1.2.11. Question score: The sum of the three presentation scores for a relevant question.

1.2.12. Sub-test score: The sum of the two relevant question scores.

1.2.13. Sub-test decision: The decision for a sub-test.

1.2.14. Examination decision: The decision for the entire examination (both sub-tests).

1.2.15. Phase I: Pre-test interview

1.2.16. Phase II: Data collection

1.2.17. Phase III: Data analysis

1.2.18. Phase IV: Post-test interview

1.2.19. Multiple Issue Polygraph (MIP): The TES format is a MIP used to assess the credibility of answers to security questions. MIP's are not an exclusive method for testing credibility because they are required to address multiple relevant issues in a single series. To maximize accuracy and utility, the *successive hurdles* model should be used when NO or SR decisions have been reached (Meehl & Rosen, 1955; Krapohl & Stern, 2003).

1.2.20. Successive Hurdles: This model is part of the CI screening process that entails the use of not just one polygraph examination, but a series of polygraph examinations, with each successive one having better specificity than the previous (Meehl & Rosen, 1955; Krapohl & Stern, 2003). For TES this means that following a post-test interview, the second polygraph examination should be a different format and more narrow in focus than the initial screening exam. In order to accomplish successive hurdles correctly the polygraph examiner must have intimate knowledge of the essential elements for each security topic.

1.2.21. Credibility Assessment: This is a multi-disciplinary field of existing, as well as potential techniques and procedures to assess truthfulness. Credibility assessment relies on physiological reactions and behavioral measures to test the agreement between an individual's memories and statements.

1.2.22. CI Screening Process: This process begins with the pretest interview (Phase I) and continues until all security issues are resolved. The CI screening process can take several days depending on whether examinee continues to provide reportable information. The successive hurdles model identified in 1.2.20 above is an integral part of the CI screening process.

1.2.23. Elicitation Interview: The word *elicitation* means to "draw out something hidden". The TES pretest interview, using non-threatening elicitation techniques provides examinee an opportunity to disclose hidden information.

1.2.24. Expanded Interview: This is an initial series MIP non-confrontational post-test interview conducted after an SR or NO decision. The Expanded Interview uses forensic

tools based on science to garner a partnership between examinee and examiner for resolving issues relevant to the salient security topic.

1.2.25. Interview Route Map (IRM): A visual representation of the aims and objectives of the CI screening topical issues (Milne & Bull, 1999). Key words on the visual map represent concepts that allow the examinee to visualize images in order to reduce cognitive load and enhance recall. The IRM is used in both the Phase I and Phase IV of the TES process and assists in eliciting reportable information.

2. Polygraph Examiners Authorized to Conduct TES Examinations

2.1. TES examinations shall only be conducted by federal polygraph examiners who have received specialized TES training at the National Center for Credibility Assessment (NCCA). Intern polygraph examiners may conduct TES examinations under the auspices of federal examiners certified to conduct TES examinations.

2.2. In the event a polygraph examiner begins but is unable to complete a polygraph examination, in most cases another examiner should not complete the examination, that day. The examinee should be rescheduled for another day, at which time another or the same examiner will conduct the examination. If a sub-test was successfully completed prior to the termination of the previous session, that sub-test need not be repeated.

3. Environment

3.1. Polygraph examinations should occur in a suitable examination room. There should be chairs for the examiner and examinee and a table for the polygraph equipment. The examination room should not contain distracting equipment or decorations, and should have a means of controlling the ambient temperature. The room may have an observation window, and at a minimum contain audio recording equipment.

3.2. Normally, no one other than the examinee and the polygraph examiner is authorized to be present in the examination room during the first three phases of the polygraph examination. An exception to this provision is the need for an interpreter. Any person granted an exception must have an appropriate security clearance for the matters to be discussed, and must agree to keep any personal information confidential.

4. Equipment

4.1. Polygraph testing may be conducted using any polygraph instrument sanctioned by the Department of Defense (DOD). Each examiner shall be required to calibrate the instrument in the manner taught by NCCA, consistent with manufacturer's specifications and in accordance with DOD policy.

5. Interviews

5.1. The TES format and questions are highly standardized to ensure consistency and reciprocity. It is not the intent of the TES process to seek out minor security violations or to identify every foreign contact. However, when such topics are revealed by the examinee they will be investigated so that they do not become a problem during the testing process. The relevant topical areas identified in 13.2.1 and 13.2.2 below are designed to elicit information which can serve either as investigative leads or to provide the basis for further interview to determine if espionage, compromise of classified information, deliberate damage to information or defense systems or terrorism had been committed. The TES elicitation pretest interview in combination with the IRM will assist in the testing process to determine if any of the relevant security issues have been committed. An elicitation interview can take place at any time during the polygraph process. Phase IV interviews (hereafter, post-test interview) is to determine why a specific relevant question(s) was significant to the examinee, and to give the examinee an opportunity to provide a reasonable explanation for the significant responses. Additional data collection should not be used in lieu of post-test interview procedures. It is recommended that the IRM be used in conjunction with the post-test interview. The IRM is a non-confrontational tool that will assist in bringing clarity to the post-test process. As with all testing, interviews are conducted in a manner that conveys respect for the examinee and is in no way degrading. Interviews of examinees during any phase of a polygraph examination will not probe any of the following areas unless these issues are revealed by the examinee as having relevance to responses or admissions made in connection with counterintelligence questions posed during the examination:

5.1.1. Religious beliefs or affiliations
5.1.2. Beliefs and opinions regarding racial matters
5.1.3. Political beliefs and affiliations
5.1.4. Opinions regarding the constitutionality of legislative policy
5.1.5. Use of drugs or alcohol (except for the purposes of assessing suitability)
5.1.6. Affiliations with labor unions
5.1.7. Sexual matters
5.1.8. Finances

5.2. The examinee may terminate the CI screening process at any time. An examinee may request legal counsel at anytime. However, counsel should not be present in the polygraph examination room during any phase of the examination.

6. Interview Terminations

6.1. Termination report: Whenever an interview is terminated before the examination has been completed, the polygraph examiner will immediately advise the appropriate supervisory

examiner and fully describe the circumstances of the termination in a polygraph report. The report must include the reason(s) for discontinuance, how much of the examination remained, whether or not adequate tests had been conducted from which a diagnostic conclusion may be rendered, the attitude of the examinee, and whether examinee is willing to continue the CI screening process later.

6.2. Examiner termination: A polygraph examiner may terminate an examination for several reasons. Examiners may assess the examinee to be mentally, physically or behaviorally unsuitable for testing. The examiner may be ill or feel unable to establish adequate rapport to conduct a valid examination. Medical problems and psychological problems involving examinees must be discussed with the supervisory examiner.

6.3. Examinee termination: An examinee may terminate an examination for several reasons. The reasons for examinee termination may be less clear than the reasons for polygraph examiner termination. Detailed notes should be taken regarding the discussion leading to the termination of the examination. If the examinee does not wish to continue the interview or resume it later, the supervisory examiner should be informed. If the examinee makes any allegations or threats, these must be noted in the polygraph report.

7. Examination Procedures

7.1. Phase I will proceed in the following manner:

7.1.1. After the appropriate introductions, the examiner will discuss the purpose of the examination and acquaint the examinee with the TES format. The following is an example of the information provided to the examinee at this time.

7.1.2. “I will be administering a polygraph examination today. This is a security examination to allow you to obtain or retain your security clearance. The polygraph examination consists of several tests. I will explain all the questions on each test before I conduct them. First, however, I need to obtain your consent to undergo this examination."

7.1.3. Appropriate administrative instructions should be provided concerning note-taking and audio or video recording. The purpose of the instructions is to ease the anxiety of the examinee and provide a rational explanation for taking notes and audio or video recording.

8. Consent to Undergo PDD Examination

8.1. If required, accomplish rights advisement first.

8.2. At the beginning of the pretest interview for the TES examination the polygraph examiner will obtain the examinee's informed consent to undergo the TES examination. The examinee's consent will be in writing before continuing the examination. The preferred method is to read the consent form to the examinee prior to the examinee signing the form. Appendix D is an example of an appropriate consent form.

8.2.1. If a second day is necessary to complete the CI screening process, another consent form will be completed. A consent form will be obtained for each new day of testing.

9. Overview of the Procedures

9.1. After obtaining consent, an overview of the polygraph procedures is given. The following is an example of the information contained in this overview.

9.1.1. "Before we continue, I would like to give you an idea of what we will be doing today. Shortly, I will be asking you some medical and health questions because I need to make sure you are suitable to be given this examination. Next, I will explain the instrument and how it works and I will demonstrate it to you. I will discuss the questions that I will be asking you on the first test. Before each test, I will discuss the questions on that test. In this way, I will be sure that you understand the topical areas and will not be surprised by any of the questions. Do you have any questions?"

9.2. Establishing Responsibility: The responsibility statement establishes the examinee's responsibility to ask questions and to tell the truth and not withhold any information. It was adapted from *Hiring the Best, Interviewing for Integrity* by Brian C. Jayne and Joseph P. Buckley (2005) with John Reid and Associates, Chicago, IL. The responsibility statement is presented during the overview or at any point in the pretest process up until after the acquaintance test. The responsibility statement can be approached in a variety of ways, but generally covers of the following information:

9.2.1. Set **the stage**: "This interview is different from most job interviews. It is about your suitability to possess or retain a security clearance. To a very great extent, this session is a *credibility assessment* of your ability to provide complete and accurate information about your background as it relates to the security questions on this test."

9.2.2. Explain **the process**: "There are two parts to this *credibility assessment*. The first part is a discussion of the test issues. The second part is when the polygraph sensors are attached to your body and your physiological activity is recorded while you answer specific and reviewed questions. To be successful in this process you must do two things."

9.2.3. Fix **responsibility**: "First, if you do not understand something it is your responsibility to ask questions until I explain the matter clearly to you. My job is to tell you what you need to know to complete the test successfully. I will do that. Your job is to make sure you understand everything I say."

9.2.4. Encourage **truthfulness**: "Secondly, when answering my questions about the security issues you must be as thorough and accurate as possible. Do not leave matters out because they seem unimportant to you. Even minor details can be very important during this testing process. At the end of our discussion, you should be confident of the accuracy of all your statements. If you are not, then our discussion should continue."

9.2.5. Seal **the deal**: "Can I count on you to ask me questions if you do not understand something? Can I also count on you to be completely straightforward and truthful in all your statements regarding the security questions today?"

10. Medical/Biographical/Background Information and Countermeasures Statement

10.1. After the Consent Form is signed, sufficient medical, biographical, and background information is obtained to assess the suitability of the examinee to undergo the examination and to help establish rapport with the examinee as taught at NCCA. Sufficient background information should also be obtained (without laying a foundation and setting comparison questions) that will easily allow the polygraph examiner to move from a Directed Lie Comparison (DLC) format to a probable lie comparison (PLC) format if required. Lifestyle questions are not allowed during this interview process.

10.2. Countermeasures statement: It is important to provide some form of countermeasures statement to make the examinee aware that non-cooperation or deliberate efforts to influence testing will adversely affect the examination process. There are a number of approaches to this issue. The following is one such approach:

10.2.1. "It is not uncommon for people who have to take a polygraph examination to research information on the topic. Often, they come across sites or read articles that suggest they have to perform some activity to help them through their polygraph examination. Such sites and articles often provide bogus information. In fact, when people attempt to influence the outcome of their polygraph examination in various ways, such activity reveals that they have abdicated their responsibility to tell the truth and are being non-cooperative. Can I count on you not to involve yourself in such activity?"

11. Explanations of Instrumentation and PDD Theory

11.1. During the pretest interview explain the instrumentation and fight or flight as it relates to polygraph. The following is a basic guideline for these explanations.

11.2. “You may be a little nervous, especially if you have never had a polygraph examination. To help put you at ease, I will explain what the instrument is, and how it works. The polygraph is a diagnostic tool used to determine if you are telling the truth. It simply records physiological changes taking place in your body when a series of questions are asked. Changes in your respiration, sweat gland activity and heart activity will be recorded. Please notice the two rubber tubes. One will be placed across your chest and the other will be placed around your abdominal area. They will monitor and record your respiration. The two metal fingerplates will be attached to two of your fingers and will monitor and record changes in your sweat gland activity. The blood pressure cuff will be placed on your arm and will monitor and record changes in your cardiovascular activity. During the test, I will inflate the cuff with air, so you may feel some pressure on your arm. Finally, the pad in the chair is designed to pick up body movements. When the polygraph test begins, please do not move unless instructed to do so.”

11.3. “The physiological changes recorded by the various components are a result of your body’s autonomic response system. You have no control over this response system. For example, visualize yourself walking down a dark alley late at night. Suddenly you hear a loud noise. You will instantaneously decide either to remain where you are and investigate the source of the noise, or to flee the area, sensing danger to your well-being. Regardless of the choice you make, your body automatically adjusts itself to meet the needs of the situation; your heart may beat faster, your breathing may change and you may break out in a cold sweat.”

11.4. “Your body produces the same type of physiological responses when you deliberately choose to lie or conceal information. Our parents, grandparents, relatives, and teachers all taught us that lying, cheating, and stealing are wrong. Think about the first time you were caught lying. Remember how your body felt during that confrontation. Your heart may have been racing or you may have been sweating. However, the responses were automatic; your body adjusted to the stress of the situation.”

11.5. “People are not always 100% honest. Sometimes it is more socially acceptable to lie than to be honest - such as telling people you like their clothes when you really do not. It is important for you to understand that even though a lie might be socially acceptable, a small lie, or a lie by omission will cause your body to automatically respond. The recording on the polygraph will show only the physiological responses. I cannot know what kind of lie you are telling. Therefore, it is extremely important that you be completely honest to the security questions that I will be asking you. Remember, it is your responsibility to ask me questions if you do not understand something and to be completely honest and thorough when discussing the security questions on this examination.”

12. Acquaintance Test

12.1. A standard known solution numbers test will be the only acquaintance test used. The acquaintance test will cover the following three topics: "I am now going to demonstrate the physiological responses we have been discussing. (1) This test will give you the opportunity to become acquainted with the recording components (2) it will give me the opportunity to adjust the instrument to you before the actual test (3) it reflects you are able to follow my instructions. (4) In addition, this test will demonstrate to me that you are physiologically capable of responding “when you tell a lie."

12.2. The standard polygraph components are attached followed by the acquaintance test. The acquaintance test should be conducted in the manner taught at NCCA.

12.2.1. The acquaintance test provides the polygraph examiner with an opportunity to adjust the components to examinee’s physiology and to make sure that movement sensors and other components are working appropriately.

12.2.2. The movement sensor should contain sufficient sensitivity so that unsolicited movements can be readily identified.

12.2.3. Test data cannot be accurately analyzed if there is insufficient sensitivity in the various components therefore before entering operation, each component should contain appropriate sensitivity as taught at NCCA.

12.3. Following the acquaintance test, the polygraph examiner should take the opportunity to acknowledge the results in a manner similar to the following:

12.3.1. “That was excellent. It is obvious that you know lying is wrong and it is clear that you are capable of responding when you tell a lie. You reacted strongly when you lied about that number. Even though the number was unimportant and the lie insignificant, you still responded. I am also able to see where you told the truth. That will make this examination very easy to complete as long as you follow my directions and are 100% truthful to the security questions.”

12.3.1.1. Prior to verbally acknowledging the results of the ACQT, the polygraph examiner should conduct a global review of the test data. The review will reveal whether there is adequate sensitivity in the components, if the test data contains abnormal nervous tension, whether examinee reacted at the key, and whether there is atypical physiology indicative of countermeasures activity.

12.3.1.2. The global review may dictate what approach the polygraph examiner might take when verbally acknowledging the results of the ACQT. The test data itself is normally not shown to the examinee.

13. Question Review

13.1. The Intelligence Community Policy Guidance 704.2 outlines the security information of importance for Counterintelligence Scope Polygraph (CSP) examinations. The following topical areas must be covered in order to have reciprocity between polygraph programs.

13.1.1. The following topical areas establishing reciprocity are:

- Involvement with a foreign intelligence service (FIS), foreign security service (FSS); Involvement in espionage.
- Terrorism.
- Foreign contacts.
- Protection of classified information.
- Damaging/sabotaging government information systems, clandestine collection (reconnaissance or other collection systems), or defense systems.

13.1.2. DOD polygraph programs may tailor their security questions to fit the needs of their customers, as long as the questions and the scope of the questions are sufficient to meet reciprocity requirements.

13.2. The TES format as taught at NCCA uses two sets of relevant questions. One set of relevant questions used in Sub-test A, and the second set of relevant questions used in Sub-test B.

13.2.1. Sub-test A:

R1. **Have you (*deliberately*) damaged any US government (USG) information or defense systems?**

R2. **Have you been involved in espionage or terrorism against the United States?**

13.2.2. Sub-test B:

R3. **Have you (*deliberately*) mishandled any classified information?**

R4. **Have you had any unauthorized foreign contacts?**

13.3. Sub-test A should be conducted first unless the examinee has an issue relating to Sub-test B topical areas.

13.4. If significant information is provided during the pretest interview regarding a security topic, the preferred method is to move directly to a breakdown test to resolve that security issue.

13.4.1. There is no definitive rule as to when a polygraph examiner should go directly to breakdown testing. The key phrase to consider is ***significant information***. This is reportable information directly related to the discussed security topic(s). It is information that should be fully resolved before testing of multiple issues can continue.

13.4.2. In cases where polygraph examiners obtain information prior to initial testing, a relevant question may be worded to qualify the question in the initial test. If examinee is, SR to the qualified question the polygraph examiner should use the information already obtained as an aide to elicit a reasonable explanation for the responses evident during the testing.

13.4.3. No matter which method is used, the solution is the same – eliciting information. No amount of data collection will replace a good elicitation interview.

13.5. Each security topic must be thoroughly discussed with no shortcuts taken. This means that in addition to a definition for the relevant question, the polygraph examiner should discuss all of the essential elements for the particular security topic, and provide an appropriate number of appeals and topic clarification questions so there is no doubt in the examinee's mind what the security topic encompasses.

13.6. Appendix A (Scoping Guide) provides definitions, essential elements and clarification questions for the relevant questions listed in 13.2.1 and 13.2.2 above.

13.7. Appendix B (DLC questions) provides acceptable DLC questions and irrelevant questions for NCCA students.

13.8. Polygraph examiners may employ minor variations of relevant questions to assure understanding by examinee or to accommodate explanations or admissions by the examinee as set forth in Appendix C (Alternative Relevant Questions). It is important that the minor variations not change the scope of the relevant issue being tested.

13.9. During the question review, it is recommended that the polygraph examiner take the examinee out of the components and move examinee to a different chair while conducting the elicitation pretest interview. Keeping examinee attached to the components is not conducive to rapport building. If there is a requirement to keep examinee in the polygraph chair (i.e. due to camera angle) it is suggested that the components be taken off the examinee and that the polygraph examiner position himself or herself to where there are no barriers (i.e. chair arm) between the examiner and examinee making observation of withholding behavior, and elicitation of information extremely difficult.

13.9.1. It is important to remember that the pretest interview should be a dialogue not a monologue. A dialogue requires an exchange of information. It is the examinees' responsibility to ask questions when they do not understand something and to be honest and thorough in their answers to security questions. However, it is the polygraph examiner's responsibility to conduct an interview that allows the examinee an opportunity to provide information, even if it is minor. When polygraph examiners deliberately place a barrier (e.g. table corner, chair arm, etc.) between themselves and the examinee the barrier often hampers the exchange of information.

13.9.2. Ideally, the polygraph examiner and the examinee should be sitting in similar chairs at a ten o'clock two o'clock position. This position is non-confrontational and assists in partnering with the examinee.

13.10. Explanation to the examinee: "I am going to review the questions that I will be asking you during the examination. There are three types of questions; security questions and two types of diagnostic questions. I will explain each type of question and I will review each question in detail. It is very important that you pay attention and carefully follow directions. The first questions will be the security questions. Remember, it is your responsibility to ask me questions if you do not understand a security issue we are discussing, and it is also your responsibility to be thorough and straightforward in your answers to the security questions."

13.11. Review Sacrifice Relevant. The sacrifice relevant question may be reviewed as the first relevant question or as the last (third) relevant question.

13.11.1. The rationale for the sacrifice relevant question might be as follows: (e.g., I need to make sure you intend to be truthful to the security questions we are going to review *(we just reviewed)*, so I am going to ask you: (Either sacrifice relevant can be used):

- Do you intend to answer the security questions truthfully?
- Regarding the security questions, do you intend to answer truthfully?

13.12. Pretest of relevant questions: Pretest only the relevant questions for the sub-test you are conducting.

13.12.1. Appendix A provides a scoping guide with the elements that must be covered for each security topic. It is important to note that "information" is the key to any CI screening examination. Initial admissions to security violations may be hiding serious reportable information.

13.12.2. Do not short cut the interview process. The review of the relevant issues must be detailed with sufficient appeals and topic clarification questions to provide examinees opportunity to fulfill their responsibility to ask questions if they do not understand something and to provide information that is relevant to the security issues.

13.12.3. Reading a pretest interview from a script, memorizing a script and repeating it, or using a checklist does not create dialogue. Such habits are unacceptable and strongly discouraged. It is recognized that TES is a structured interview and there are certain detail that must be stated during the process (e.g. during the ACQT and setting up the DLC questions), however these structured comments should be part of the overall dialogue and not a memorized script recited as a monologue. Appendix F contains a TES outline for NCCA students to use until they develop their own style and become proficient in their understanding of the CI issues covered by the relevant questions. The TES outline is not a crutch and is not memorized as a script. Such actions discourage dialogue and hamper the ability to obtain information.

13.13. Rationale for directed lies: The following is an example containing one approach to introducing the diagnostic questions:

13.13.1. “I am now going to discuss the second type of questions, we call them diagnostic questions. As I explained earlier, when you tell a lie your body responds and I will be able to see it; just as I did during the acquaintance test. For various reasons (sick, tired, using some medication, etc.) some people lose their capability to respond. Consequently, during testing I will ask some questions to make sure you retain the capability to respond when you lie. Additionally, these questions will require you to pay attention and answer as we reviewed”.

13.13.2. “First, I will review those questions used to determine if you are capable of responding when you tell a lie”. I already know the answer to these questions because we all have done these things at one time or another. When I ask the question I want you to think of an occasion when you did this - do not tell me about it; just think of a specific time. Then lie to me and say NO."

13.13.3. A list of DLC questions is located in Appendix B.

13.14. Review of DLC questions

13.14.1. Each DLC question should be introduced by pointing out that the event, i.e., violation of a minor traffic law, etc., is one that most people have done. For example, “We have all violated a minor traffic law at some time in our life, I’m sure you have haven’t you?” At this point, the polygraph examiner will want to observe an affirmative nod or hear a verbal yes from the examinee. Provide instructions to make sure examinee has a specific event in mind explaining that he or she does not need to provide any specific details of the event. Let the examinee know that the test question on the test is, “Did you ever violate a minor traffic law?” Provide instructions that the examinee simply recognize the question as one to which he is lying, and to answer in a timely manner.

13.14.2. It is critical that the polygraph examiner make sure that the examinee has a specific incident in mind when lying to the DLC, as cognitive processing accounts for a major portion of the response to the question. This is accomplished during the pretest development and review of the DLC questions, as indicated above. It is equally important for the polygraph examiner not to force examinee to think about or dwell on the DLC question during question presentation in the data collection phase. When examinee answers a DLC question, the answer should be as timely as the answers to the relevant and irrelevant questions.

13.14.3. Review two directed lie comparison questions from the list in Appendix B. Do not give any examples of what you mean or what would be included in the DLC question. The impact of the DLC will be stronger if it comes to mind naturally, than if you force it into their minds. Similarly, if there is any resistance to a DLC (e.g. the examinee claims never to have engaged in the activity) do not use it - select another DLC.

13.15. Rationale for and review of the irrelevant questions.

13.15.1. “The final diagnostic questions you may hear are those you will answer truthfully so that I can see how you are responding when you tell the truth. It will be obvious that you are telling the truth. The questions are...."

13.15.2. Review two irrelevant questions from the list in Appendix B.

13.16. Question Re-review.

13.16.1. Re-review all questions and have examinee answer as he or she would during the phase II. Questions should be reviewed in the following sequence: SR, R1, R2, C1, C2, I1, and I2. If the examinee answers a DLC question incorrectly, remind the examinee to answer the question with a “no” answer, thus lying to the question. Repeat the review until the examinee does it correctly.

13.17. Examinee Instructions

13.17.1. Instruct examinees that they will be hearing some or all of the questions, and that the questions will not occur in any specific order. Inform them that some of the questions will be repeated and they should sit still and follow directions. Remind examinees that they are to deliberately lie to the set of reviewed diagnostic questions designed to make sure they have the capability of responding when they lie. When they hear those questions, they should recognize the question, answer with a lie, and wait for the next question. The examiner will not instruct the examinee to visualize, concentrate on, or playback in his or her mind, the event in question while answering in-test.

14. Phase II

14.1. Question Sequence

14.1.1. Sub-test A: I1 I2 SR 1C1 1R1 1R2 1C2 2R1 2R2 2C1 3R1 3R2 2C2

14.1.2. Sub-test B: I1 I2 SR 1C1 1R3 1R4 1C2 2R3 2R4 2C1 3R3 3R4 2C2

14.2. Notations

14.2.1. "Stim marks" are used as taught by NCCA. The questions are annotated using the notations above. The first relevant question is annotated R1, the second comparison is annotated C2, etc. It is not necessary to indicate the number of the presentation (e.g. the 2 before R2 on the second reading of R2).

14.2.2. Question spacing will be between 20 and 30 seconds. Spacing should vary within the window so that a set pattern is not established. Irrelevant questions may be inserted for the purposes of allowing physiological responses to return to baseline (obtaining homeostasis). Only one irrelevant may be inserted to return examinee to baseline. If examinee does not return to baseline following insertion of the irrelevant question, go out of operations. In other words, you will not ask multiple irrelevant questions in succession. However, during the course of the chart you may insert up to three irrelevant questions, as long as they are not consecutive presentations (excluding the first two irrelevant questions).

14.2.3. The test is run once (one chart). If an artifact (affecting two out of the three physiological parameters, i.e., both respiratory and EDA or EDA and Cardiovascular) occurs during one of the relevant questions or a relevant question is not able to be evaluated due to movement, examiner error, etc., do NOT repeat the question, at that point. The examiner has two options.

14.2.3.1. If the artifact is noticed while the test is being conducted, the examiner may add a fourth presentation consisting of three questions (4R1, 4R2 and 3C1) to the end of the test.

14.2.3.2. If the artifact is noticed after the test is completed, conduct a short test as follows: I1 I2 SR C1 R1 R2 C2. The examiner will go out of operation before running the short test. Explain, to the examinee, that there were artifacts and continued testing is necessary. The short test should be labeled A-1S or B-1S, etc.

14.2.4. Even though the artifact occurred at only one relevant, both relevant questions must be asked. However, only the relevant question that contained the artifact will be evaluated. The score for the repeated (artifact) relevant question will be added to the total of the two previously presented relevant questions to provide a total of three presentations of the relevant question.

14.2.5. If an examinee answers "yes" to the first DLC question (1C1), the examiner should go out of operation. If the examinee answered incorrectly, the examiner should discuss the testing procedure with the examinee to make sure he or she understands the procedure. Remind the examinee to "lie" by answering "no" to those questions. Begin the test again.

14.2.5.1. If an artifact occurs at 1C1 the examiner may stop or continue the chart based on the artifact. If the artifact appears to be an apparent attempt at countermeasures (e.g. the movement sensor contains a response indicating a physical movement), the polygraph examiner can continue the test to see if frequency and specificity occurs.

14.2.5.2. If the polygraph examiner chooses this option and frequency and specificity occur a post-test interview should follow providing the examinee an opportunity to explain the non-cooperative behavior.

14.2.6. If the examinee answers "yes" to any of the other DLC questions during data collection, give answering instructions (AI) but do not repeat the question. Continue with the test. In either case, that DLC question may <u>not</u> be used for scoring.

14.2.7. If both comparison questions in an analysis spot contain artifacts or are answered incorrectly, thereby precluding analysis of one repetition of the relevant questions, the evaluation conclusion will be No Opinion. The entire sub-test will be conducted again. The rationale for this decision may be any of the following:

14.2.7.1. If examinee continues to answer the DLC questions with the wrong response it may because the examinee is distracted and not focusing on the test, or there is the possibility that the examinee is being non-cooperative.

14.2.7.2. If artifacts are only at the DLC questions, there is the possibility of countermeasures activity. If artifacts appear throughout the test the possibility exists that examinee is being non-cooperative, is hiding information regarding the relevant issues, or has an outside issue that needs to be resolved. It is up to the polygraph examiner to discuss the behavior in a post-test environment and take corrective action.

15. <u>Phase III</u>

15.1. Both research and anecdotal field data obtained during the past two decades reveal that an evaluation of PLC or DLC test data from any CSP format should be conservative. The initial review should be global with the polygraph examiner questioning any anomalies present.

15.1.1. When a proper pretest interview is conducted, using the techniques presented in this pamphlet, yet the test data is erratic and contains excessive nervous tension this may suggest the examinee has not fulfilled his or her responsibility to reveal information relevant to the security issues.

15.1.2. When the first sub-test contains stable tracings that are relatively simple to evaluate, but the second sub-test is erratic with what appears to be excessive nervous tension this may also suggest the examinee has undisclosed information.

15.1.3. When the global review discloses atypical physiology in the test data, particularly with frequency and specificity it may suggest non-cooperation on the part of examinee. Non-cooperation on the part of the examinee is often the result of examinee withholding relevant information about the security issues.

15.1.4. After a numeric evaluation, the polygraph examiner should continue with a global review looking for inconsistencies between the global review and the numeric score. For example, if the vertical numeric score at one question in a sub-test is a +1 and the other vertical numeric score at the second relevant question is a +6 with a combined horizontal score of +7 this would be called NSR in the TES format. However, a global review will most likely reveal consistent, significant responses at the relevant question in the +1 spot suggesting salience to the examinee. The polygraph examiner should conduct a polite post-test interview providing examinee an opportunity to explain the significance of the question.

15.2. Initial TES research used the 7-position scoring system, but added some safeguards to improve accuracy particularly when identifying deceptive examinees. For example, if after evaluating the test data the final score fell into the NO range, the first presentations of both relevant questions are evaluated against 1C2: 1C1 is ignored. This simple conservative approach often moved the NO opinion to a conclusive result and more importantly improved the accuracy of deceptive decisions without affecting the non-deceptive decisions. Additionally, if the final decision is still NO, a post-test interview should be conducted giving the examinee opportunity to fulfill his or her responsibility as outlined in this pamphlet.

15.2.1. The appropriate evaluation for TES is the 7-position scoring system as taught at NCCA with the safe guards outlined in 15.2 above. If either of the vertical question totals is lower than or equal to -3 the decision is SR. If the horizontal total is lower than or equal to -4 the decision is SR. If the horizontal total is greater than or equal to +4 with plus scores in both vertical spots the decision is NSR. Any other total is NO.

15.3. The NCCA is not averse to using the 3-position scoring system as a conservative evaluation process for TES. The information in 15.1.1 through 15.1.4 still applies. Appendix G contains a copy of a TES evaluation sheet.

16. Phase IV

16.1. Upon completion of the test data analysis (TDA) phase, the examiner will conduct a post-test interview notifying the examinee of the results of the polygraph examination. When significant responses are observed at relevant question(s), a line of questioning begins with the purpose of gathering information to explain the unresolved issues relevant to the matter under investigation. For NSR, the examinee is informed of a preliminary opinion of truthfulness to the relevant issue and this opinion remains preliminary until a quality control review is conducted. In the case of a NO examination, the examinee is advised the examination has not met the criteria of a conclusive examination, therefore the relevant issue is unresolved and further testing is necessary. Further polygraph testing is not accomplished until examinee is thoroughly interviewed to determine why conclusive results were not obtained.

16.1.1. Upon completion of a thorough interview to determine why conclusive results were not obtained, the polygraph examiner using the successive hurdles model, should breakdown the relevant question containing the most significant responses. The breakdown test should cover the essential elements for that relevant topical issue. The polygraph examiner has the option of conducting a second TES examination as outlined in paragraph 16.5 below.

16.2. NSR Decision: The polygraph examiner's NSR decision means the testing for that sub-test is complete. After completion of sub-test A; sub-test B will be conducted (or vice versa if "B" was conducted first). Upon completion of sub-test B (and both sub-tests resulted in NSR decisions), the examinee will be informed that the tests are subject to further review prior to reaching a final determination of results and that it is sometimes necessary to administer additional tests to confirm the original decision. Determine if the examinee would be willing to return for additional testing, if necessary.
Appendix E provides an example of how to transition from sub-test A to sub-test B.

16.3. SR Decision: If, following the evaluation of sub-test data, there is a need to resolve a security topic due to significant responses or other actions of the examinee, i.e., deliberate artifacts in the physiological responses, the examiner will immediately conduct a thorough post-test interview. The significant responses to the relevant questions generally indicate that the examinee withheld information during the pretest interview. It is the polygraph examiner's responsibility to give examinee opportunity to provide a reasonable explanation regarding the significance of the question(s).

16.3.1. If the strongest responses are at a particular relevant question, the polygraph examiner should let the examinee know that the interview will be expanded covering the significant security topic. The expanded interview is a non-confrontational interview giving the examinee an opportunity to provide a reasonable explanation for the responses. The IRM is used with the Expanded interview as part of the elicitation process.

16.3.2. There is concern among some in the polygraph community that significant responses at one relevant question does not mean examinee committed an act involving that particular relevant issue. (E.g. Significant responses on sub-test A to espionage and terrorism when the real issue is mishandling classified information covered later in sub-test B). This should not concern the polygraph examiner. The examinee chose the espionage and terrorism question on which to respond. It is up to the examinee to provide the explanation. The expanded interview will provide examinee an opportunity to explain the responses and breakdown testing using the successive hurdles model will resolve whether examinee is being truthful in his or her responses. Breakdown testing does not, and should not replace a good post-test interview.

16.4. If the relevant issues have been fully explored as laid out in the scoping guide (Appendix A), and topic clarification questions have been correctly asked, and examinee behavior correctly analyzed, it is reasonable to assume that examinee is withholding information. A good polygraph examiner can be polite, yet effective at obtaining reportable information.

16.5. On the other hand, if shortcuts were taken, all the relevant topical areas were not fully explored, the polygraph examiner misread examinee's behavior, or examinee had some outside issue not brought to the attention of the polygraph examiner, it may be possible that the significant responses in a NO test are anomalous. This should be the exception not the rule. A post-test interview should be conducted to see what the polygraph examiner missed during the pretest interview. After the post test interview, if the polygraph examiner still feels any of the above occurred, the examiner may attempt to resolve the problem rerunning the test using the TES format with different DLC questions. However, if the polygraph examiner feels examinee is withholding information the post-test interview should continue. After completion of the post-test interview the issue should be resolved using the successive hurdles model.

16.6. If examinee makes admissions directly related to the relevant question(s) explicit detail (who, what, where, when, how, why) should be obtained. Consider taking a signed statement, or during the summarization of the information take written notes and have examinee sign and date the notes. Breakdown testing should be conducted to test the credibility of the examinee's statements. The particular relevant security topic is not resolved until all of the essential elements covering the relevant topic are covered.

16.7. Once the deceptive relevant issue(s) is resolved, a clearing test should be conducted on the other question(s) in the sub-test before moving to the next sub-test. The clearing test can be in a PLC or DLC question format and should cover all the essential elements for that relevant topic. If the clearing test yields a DI/SR decision, a post-test interview should follow. There should not be additional polygraph testing until substantial information is obtained. If the clearing (confirmatory) sub-tests continue to yield DI decisions with substantial admissions between testing the testing process can continue, as long as the examinee is agreeable to further testing and his or her physiology is still responsive. Extended testing should include appropriate

breaks (e.g. lunch, restroom, water, smoking, etc.). If an examinee must return for further testing, a minimum of 24 hours from time of release must elapse before he or she is re-tested.

16.7.1. The point of paragraphs 16.3 through 16.7 above is that continued testing should only occur when significant information is obtained during the post-test interview. The solution is reportable information. As stated before, testing should never replace a good interview. There is a very strong danger of habituation when a polygraph examiner chooses to conduct repeated tests on the same issue when no information has been obtained or a credible post-test interview not conducted.

16.7.2. Regardless of which sub-test is administered the second sub-test may NOT be administered if the first sub-test has not been resolved. This does not preclude the polygraph examiner from expanding the post-test interview to topics covered in the second sub-test area.

16.7.3. When there is an absence of reportable information forthcoming from the examinee the polygraph examiner should follow the successive hurdles model.

16.8. NO Decision: If, following the evaluation of the sub-test data, a conclusive decision cannot be rendered due to *inconsistent* responding to the relevant questions, the polygraph examiner will conduct a thorough interview to determine what was significant about the relevant question(s). The criteria for continued testing with an NO decision are the same as the criteria for continued testing with an SR decision. If examinee does not provide a reason for the inconsistent responses, the most significant relevant question should be broken down using the successive hurdles model. The maximum number of series to resolve an issue without examinee providing information between series is four for subtest A and three for subtest B. The maximum number of series only applies if the successive hurdles model is being properly followed. Due to habituation, the accuracy of the results of any additional testing is questionable.

16.8.1. The provisions of paragraph 16.5 apply if the polygraph examiner chooses to conduct another TES exam (providing the NO is after the initial series).

16.9. If the NO decision is due to an *absence of responding* to the relevant and comparison questions, consideration should be given as to whether examinee is taking medication or has a health issue that might mask physiological responses, or has taken some deliberate action to conceal physiological responses.

16.9.1. A post-test interview should be conducted to determine the reason for the absence of responding. If further testing is considered it should be after the relevant issues are fully explored.

17. Breakdown Testing.

17.1. The TES was not designed to be a stand-alone testing format. The TES sub-tests contain multiple security issues with many elements. SR responses to the relevant issues should be expected in some cases. When SR or NO decisions occur, it is expected that the polygraph examiner will conduct sufficient interview to offer the examinee an opportunity to provide a reasonable explanation for the responses. Examinee's explanation may dictate the direction of the breakdown testing.

17.2. Breakdown testing will be accomplished using successive hurdles in the manner taught at NCCA. It is important to realize that breakdown testing is still part of the CI screening process. The focus of breakdown testing is to determine a direction for further interview. This requires an intimate understanding of the essential elements for each security topic.

17.2.1. If an examinee has chosen to negate his or her responsibility to be truthful, a proper breakdown test will provide the polygraph examiner with a direction for more focused interviewing. The focus of initial breakdown testing should be in the areas covered in 17.3 through 17.7 below.

17.3. **Essential elements for damage to USG Information Systems**:

17.3.1. Unauthorized access to cause damage.

17.3.2. Physical damage.

17.3.3. Uploading a malicious code.

17.3.4. Unauthorized altering to cause damage.

17.4. **Essential elements for damage to USG Defense Systems:**

17.4.1. Weapon systems damage.

17.4.2. Reconnaissance program damage.

17.4.3. Damage to computers connecting, controlling or operating a Defense System.

17.4.4. Damage to peripheral equipment used to maintain USG Defense Systems.

17.5. **Essential elements for Espionage (Concealed FIS or FSS contact)**:

17.5.1. Unreported approaches or pitches.

17.5.2. Offering or volunteering to engage in espionage.

17.5.3. Recruitment for espionage activity.

17.5.4. Training provided by a FIS/FSS for espionage activity.

17.5.5. Tasked to obtain something for a FIS/FSS.

17.5.6. Improper copying, removing, transporting and storage of classified for espionage purposes.

17.5.7. Compensation for espionage activity.

17.5.8. Spotting and assessment activity for a foreign entity.

17.5.9. Knowledge of espionage activity that is being deliberately concealed from your agency.

17.6. **Essential elements for foreign or domestic terrorism**:

17.6.1. Member or previous member of any terrorist organization.

17.6.2. Providing support to any terrorist organization.

17.6.3. Concealing contact with any terrorist organization.

17.6.4. Taking part in or knowledge of any terrorist act.

17.7. **Essential elements for protection of classified information**:

17.7.1. Providing classified information to an uncleared US citizen.

17.7.2. Providing classified information to the media or press.

17.7.3. Providing classified information to a foreign national.

17.7.4. Unauthorized removal and storage of classified information.

17.8. **Essential elements for unauthorized foreign contacts**:

17.8.1. Unreported business contact.

17.8.2. Unreported professional contact.

17.8.3. Illegal or criminal contact.

17.8.4. Close personal contact.

Appendix A
Scoping Guide for Relevant Questions

TES Sub-test A:

- Interview Route Map should be used with the elicitation interview process while scoping the questions below.

R1: Have you deliberately damaged any US government information or defense systems?

Security 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 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.

Conditions that could raise a Security Concern:

- Illegal or unauthorized entry into any information technology system or component thereof
- Illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware, in an information technology system
- Use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system
- Downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system
- Unauthorized use of a government or other information technology system
- 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
- Negligence or lax security habits in handling information technology that persist despite counseling by management
- Any misuse of information technology, whether deliberate or negligent, that results in damage to the national security

Question Definitions:

United States Government (USG) information system: Information technology systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

USG Defense systems: Refers to military weapon systems and anything used by the USG in the nation's defense to include reconnaissance programs.

Elements: Damage to USG Information Systems:

- Unauthorized access to damage a USG Information Technology System (ITS):
    - Exchanging USG computer passwords. For what purpose? How often?
    - Misuse of USG systems such as pornography, managing a personal business, piracy, etc.
    - Hacking into a USG computer system.
    - Accessing for the purpose of damaging

- Physical Damage to a USG ITS.
    - Deliberate and intentional damage.
    - Pouring acid or other liquid into an ITS.
    - Breaking hardware, firmware, or other components of an ITS with a hammer or other tool.
    - Sabotaging [bomb, arson, etc] an ITS.

- Uploading a malicious code into a USG computer
    - Purposeful, malicious efforts to do harm to a computer system;
    - Deliberately placing malicious code into USG hardware, software, or firmware for the purpose of obtaining classified information in an unauthorized manner or damaging a USG ITS.

- Unauthorized altering information in a USG computer.
    - Changing or deleting classified information in a database without proper authorization.
    - Use of "back doors" or other surreptitious computer methods to read or change restricted data, such as someone else's email or someone else's classified information.
        - Entering someone else's compartmented data in another system, or within the same system.

- Altering a USG computer to accept unauthorized hardware.

<u>Topic clarification</u>: The following non-assumptive questions may be used during the pretest interview to clarify the security topic for damage to USG information systems:

- **Have you used a USG computer to transfer classified information to any unauthorized person?**
- **Have you downloaded any classified information from a USG computer without proper authorization?**
- **Have you "hacked" into a USG computer?**
- **Have you intentionally introduced a malicious code (*time bomb, worm, backdoor, Trojan horse*) into a USG computer?**
- **Have you deliberately damaged a computer or its components in any manner (*beating with a hammer, pouring liquids, acids or abrasives into any component*)?**
- **Have you used authorized USG computer access to commit any crimes?**
- **Have you altered information in a USG computer without authorization?**
- **Have you given your USG computer password to anyone?**
- **Have you intentionally exceeded authorized use on any USG computer?**
- **Are you concealing any unauthorized use of a USG computer?**

Definition Damage to USG Defense Systems:

- A USG <u>defense system</u> refers to military weapon systems and anything used by the USG in our defense to include reconnaissance programs. *(Since Information Systems and Defense Systems are interrelated make sure the examinee understands this question is related to <u>defense</u> and <u>military weapon</u> systems only).*

    - Equipment associated directly with the security of the USG, its military forces, or its borders, embassies, and territories.
    - Offensive or defensive weapon systems whether floating on or under the water, sitting or traveling on land, flying in the air, or orbiting in space.
    - Peripheral equipment used to interconnect these weapon systems.
    - The term *deliberately damaged* means intentional or premeditated acts.

        - These acts would result in equipment not being available or functioning properly should they be immediately needed for their offensive or defensive role.

- The question may include, but is not limited to *sabotage*. Sabotage is an act to harm the USG and/or help another nation militarily by deliberately damaging a USG defense system.

    - The method of sabotage can be complex such as altering computer code or introducing a malicious code into a defense system.

    - The method of sabotage can be basic such as cutting wires in a defense system or deliberately breaking a piece of peripheral equipment causing the defense system to fail.

- Types of Defense Systems:

    - Space Systems: (Communications, Navigation, Mapping, Meteorology, Imagery Intelligence, Signals Intelligence, Measurement & Signature Intelligence, Wide area/Ocean Surveillance, Missile Warning).

    - Smart Weapons: (TV/IR Guided Bombs; GPS Guided Bombs, Targeting Pods).

    - Nuclear Systems: (ICBM, SLBM, Bombers, CBW, Missile Defense, Air Defense).

    - Aircraft: (Military aircraft and aircraft systems).

    - Naval Combat Systems: (Ships and shipboard systems).

    - Land Systems: (All land based military weapon systems).

    - Intelligence Systems: (These are systems connected to Space, Air, Land, & Sea based Defense systems).

    - Missile Defense Systems:

    - Defense IT: (Battle space IT, Cyber Warfare, Enterprise IT, Information Security, Logistics IT, Networks and Spectrums.

    - C4ISR: Communications, Command and Control, Geospatial & Intelligence, Net-Centric Training, Sensors and UAVs.

- **<u>Elements</u>: Damage to Defense Systems**

    - <u>Weapon Systems</u>:

- Any weapon system orbiting in space; flying in the air; ground based systems; systems floating on the water or under water.
- The damage can be physical such as throwing a wrench into a jet engine or it can be sophisticated such as uploading a malicious code into a weapon system that uses computers in its operation.

- Reconnaissance programs:

  - Intelligence, Surveillance, and Reconnaissance (ISR) programs.
  - These can range from hand-held devices, to high altitude UAVs, to manned aircraft, to orbiting satellites.
  - The damage was intentional
  - The damage was sophisticated: Uploading malicious code, altering software or other computer data.
  - The damage could be unsophisticated: Cutting wires, breaking parts.

- Computers connecting, controlling or operating a USG Defense system:

  - Command and Control personnel use computers to connect, to control, and to operate Defense Systems.
  - Adding unauthorized software, firmware, or hardware
  - Unauthorized altering of data or deleting data
  - Physical damage to these computers
  - Uploading a malicious code into a defense system

- Peripheral Equipment used to maintain USG Defense Systems:

  - Damage was intentional
  - Damage was for the purpose of slowing down or destroying defense systems

Topic clarification: The following non-assumptive questions may be used to clarify the security topic for damage to USG defense systems:

- **Have you ever deliberately damaged any USG Defense system?**
- **Have you ever committed an act of sabotage on any equipment or property belonging to the USG?**
- **Have you introduced any malicious code into a computer that could result in damage or the slowing down of any USG defense system?**
- **Have you ever cut wires or thrown an object into any component of a USG defense system?**
- **Have you ever hacked into a computer system for the purpose of slowing down or damaging a USG defense system?**

- **Have you ever been approached or contacted to engage in sabotage activity?**
- **Has any entity not associated with the USG offered you money, training or tasked you to commit an act of sabotage?**
- **Have you been compensated for any sabotage activity?**
- **Do you have knowledge of any sabotage activity or planned sabotage activity against the USG?**
- **Have you deliberately damaged any peripheral equipment used to maintain defense systems?**

R2: Have you been involved in espionage or terrorism against the United States?

Security 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.

Conditions that could raise a Security Concern:

- Involvement in, support of training to commit, or advocacy of any act of sabotage, espionage, treason, terrorism, or sedition against the United States
- Association or sympathy with persons who are attempting to commit, or who are committing, sabotage, espionage, treason, terrorism, or sedition against the US
- 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:
    - Overthrow or influence the government of the United States or any state or local government
    - Prevent Federal, state, or local government personnel from performing their official duties
    - Gain retribution for perceived wrongs caused by the Federal, state, or local government
    - Prevent others from exercising their rights under the Constitution or laws of the United States or of any state

Question Definition:

Espionage: refers to the intentional unauthorized release of classified information or material to a foreign government, power, group or organization with an intent or reason to believe that the information or material may be used to the injury of the USG or to the advantage of a foreign government, power, group or organization.

An element of espionage is the unreported personal, professional or business contact with a representative of any foreign intelligence service (FIS) or foreign security service (FSS) which for any reason has been deliberately concealed and not reported. A FIS/FSS is an intelligence service or a security service of a country other than the US. A FIS/FSS can be friend or foe, allied or hostile to the USG. If the examinee is concealing such contact from you and your agency, it is unreported. Such unreported contact might involve the following:

Elements: Espionage:

- Unreported approaches or pitches by a FIS/FSS to engage in espionage.
    - A FIS normally 'spots' a potential intelligence asset (target) then 'assesses' the target to see if they have access; will be cooperative; and can be exploited. If the assessment is positive the potential asset will be approached by a representative of a FIS and asked to work for them.
    - Thus the importance of reporting such approaches.

- Offering or volunteering to engage in espionage.
    - Aldrich H. Ames is an example of someone that walked into the Russian Embassy and volunteered to work for them.

- Recruitment for espionage activity.
    - Once a FIS approaches a target and asks the target to work for them, if the target agrees to work they are recruited and become an asset or agent.

- Training provided by a FIS/FSS for espionage activity.
    - Training in Tradecraft.
    - Tradecraft is practical skills used by agents/assets in the performance of their duties.
    - In particular tradecraft enables a spy to communicate with an IO without arousing the suspicion of US Counterintelligence.
    - Tradecraft: Planned routes; Dead letter box; Secret writing; Toiletries with false compartments; Recording devices; Transmitters; Listening devices; Concealed cameras, etc.

- Tasked to obtain something for a FIS/FSS.
    - This involves a FIS telling the asset (spy) what information they want.
    - Tasking involves specific requests for the asset to do certain things.

- Improper copying, removing, transporting and storage of classified information or material for espionage purposes.

    - This is the illegal removal of classified material and concealing it at an unauthorized location.
    - The purpose of the removal is to provide the classified material to a FIS.

- Compensation for espionage activity.

    - Money, Jewelry, Diamonds, Property
    - Need for recognition; Prestige; Rank
    - Anger or Revenge
    - Thrill and excitement
    - Shared affinity with a culture, race, religion, or nation; Sex

- Spotting and assessment activity for a FIS/FSS.

    - Providing a FIS with the names of prospective assets
    - Providing a FIS with the weaknesses of a prospective asset

- Knowledge of espionage activity that is being deliberately concealed from your agency.

    - Personal knowledge of someone committing espionage that is unreported.

Topic clarification: The following non-assumptive questions may be used to clarify the security topic for espionage:

- **Have you performed any secret assignments or work for any foreign government?**
- **Have you accepted money or anything of value from a foreign government?**
- **Have you had any meetings with someone from the intelligence, military or security services of a foreign government?**
- **Have you had contact with a foreign government by phone? By email? By written correspondence? Through a third party?**
- **Have you met anyone you suspect may have been a representative of a foreign government?**
- **Have you met anyone you suspect had any official connections with the intelligence or security services of a foreign government?**
- **Have you ever been arrested in a foreign country?**
- **Have you ever been detained in a foreign country?**

Question Definition:

Terrorism: Refers to the calculated use of violence or threat of violence to induce fear and is intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious or ideological. Terrorist activity can be subversive as it interferes with, undermines, or denies individuals those rights guaranteed under the U.S. Constitution and results in or leads to the violent or illegal attempt to overthrow the U.S. Government. **(**It is important to get across to the examinee that this topic deals with terror acts directed against the USG or its people).

- Eco-Terrorism: Terrorism committed in support of ecological, environmental, or animal rights causes.
- Narco-Terrorism: Attempts by narcotics traffickers to influence policies of governments and societies through violence and intimidation.
- Domestic Terrorism: Terrorist groups born in the United States wanting to overthrow the USG.
- Foreign Terrorism: Terrorist groups headquartered in foreign countries. These organizations and groups are often supported by foreign governments. These organizations and groups have cells in the United States and are intent on overthrowing the USG as we know it.

Elements: Terrorism:

- Member or previous member of any terrorist organization.
    - Concealed or hidden from the USG, examinee's agency, and the polygraph examiner.
- Providing support *(time, money, support via computer or other information sharing)*.
    - Currency or financial securities
    - Lodging, Training, Lethal substances, Explosives
    - Communications equipment, False documents or identification
    - Safe houses, expert advice or assistance
    - Facilities or personnel, Transportation, any tangible property
- Concealing contact with any terrorist organization.
    - Hidden and unreported contact
    - Any group on the USG Terrorist watch list (e.g. Abu Nidal; Abu Sayyaf; Al-Aqsa Martyrs; Al-Jihad; Al-Quida; Salafist Group; Ansar al-Sunna; Armed Islamic Group; Asbat al-Ansar; Aum Shinrikyo; Basque Fatherland and Liberty; Communist Party of Philippines; New People's Army; Continuity Irish Republican Army; Gama's al-Islamiyya; Harakat ul-Mujahedin; Hizballah; Islamic Jihad Group; HAMAS; Palestine Islamic Jihad; Palestine Liberation

Front; Popular Front for Liberation of Palestine; Real IRA; Revolutionary Armed Forces of Colombia; Shining Path; United Self-Defense Forces of Columbia; & many others.

- Taking part in any terrorist act *(this includes knowledge of terrorist activity or planned terrorist activity)*.

    - Direct Involvement: Assassination; Bombings; Shootings; Sabotage; Ambushes; Kidnappings. Examinee is doing the action.
    - Secondary Involvement: Providing support; Acting as a lookout; Surveillance activities; Planning the acts; Unreported direct knowledge that someone is a terrorist or is planning a terrorist act.

Note: Consider the possibility of a FIS/FSS being directly involved with or providing support to terrorist groups or organizations.

Topic clarification: The following non-assumptive questions may be used to clarify the topic for terrorism directed against the United States:

- **Are you a terrorist?**
- **Have you been a member of any international terrorist organization such as Al-Qaida or Hezbollah?**
- **Have you associated with members of any known international terrorist organizations?**
- **Have you been a member of any domestic terrorist organization?**
- **Have you associated with members of any known domestic terrorist organizations?**
- **Have you provided money to any known terrorist group or activity?**
- **Have you provided personal services to any known terrorist group or activity?**
- **Do you associate with any group that advocates change in the USG by violence?**
- **Do you know anyone who is involved in terrorist activity?**
- **Have you committed any crime for political or social reasons?**
- **Have you assisted others who committed crime for political or social reasons?**
- **Are you withholding any information about your personal connection to terrorist activities?**
- **Are you withholding any information about your personal connection with any terrorist group?**
- **Are you withholding any information about your personal connection with any individual engaged in terrorist activity?**

TES Sub-test B:

R3: Have you (deliberately) mishandled any classified information?

Security Concern: Mishandling classified information: 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.

Conditions that could raise a Security Concern regarding the mishandling of classified information:

- 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
- Collecting or storing classified or other protected information in any unauthorized location
- 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, game board, hand-held "palm" or pocket device, or other adjunct equipment
- Inappropriate efforts to obtain or view classified or other protected information outside one's need-to-know
- Copying classified or other protected information in a manner designed to conceal or remove classification or other document control markings
- Viewing or downloading information from a secure system when the information is beyond the individual's need-to-know
- Any failure to comply with rules for the protection of classified or other sensitive information
- Negligence or lax security habits that persist despite counseling by management
- Failure to comply with rules or regulations that results in damage to the National Security, regardless of whether it was deliberate or negligent

Question Definitions:

Deliberately mishandling classified information: The deliberate failure to protect classified information. Removing or storing either hard copy, electronic, or memorized classified information with the intent of giving, passing, selling, keeping, or publishing that information for any reason.
This definition is also concerned with unauthorized removal of classified information or material from a secure location and long-term storage outside an approved area. This would include any transfer of classified material to a non-approved computer. This transfer would constitute long-

term storage of classified material even if the individual attempted to delete the information, because of the difficulty in deleting files from a computer.
Key Words:

- Classified refers to USG information only. There are three classifications:
    - Confidential
    - Secret
    - Top Secret (including SCI)
- Compromise:
    - Giving, passing or exposing classified USG information to any unauthorized person.
    - Unauthorized sale of classified information or material to anyone.
    - Compromise can be accomplished in two ways:
        - Revealing classified data to unauthorized persons through conversation, digital data, and hard copy.
        - Removal of classified information from authorized locations and storing in an unauthorized location.
    - Revealing classified through conversation, or unauthorized removal can be purposeful or accidental.
- Unauthorized removal of classified information involves removal of classified material from any authorized USG secure location to any unauthorized location. The definition for such removal should include:
    - Taking classified materials (documents, magnetic media, classified hardware, etc) away from a secure environment to an area such as home, garage, friend's home, or trunk of a car;
    - Entering of classified information into computerized bulletin boards or other unclassified means of communication;
    - Placing of classified information into areas where control of material is lost and the potential of compromise is increased;
    - The passing of classified secrets from one company to another;
    - Knowledge of deliberate mishandling of classified material that examinee failed to report.
- Unauthorized person refers to someone that does not hold the appropriate security clearance or does not have a need-to-know:

It is important to note that a *security violation* is not necessarily a *compromise*, but a *compromise* is always a security violation. A compromise of classified information may be hiding behind security violation admissions.

Elements: Mishandling Classified Information: Providing classified information or material to:

- Uncleared U.S. Citizen
    - One who does not have a USG security clearance.
    - One who has a USG security clearance, but does not have a need-to-know.
- Media or Press
    - Radio, TV, Magazines, Newspapers, Books
    - Computers, blogs, web-sites, bulletin-boards
    - Telephone, Email, Personal interview
- Foreign National
    - Any FN that is concealed or hidden and not reported
    - Anyone from foreign press
    - Anyone from foreign embassy, organization, group
    - Any U.S. Citizen representing a foreign group, organization, government, or country
- Unauthorized Removal and Storage
    - Removing classified from its secure environment
    - Storing at home, apartment, car, rented storage facility, friend's house
    - Downloading classified onto any unclassified medium
    - Placing classified information where control is lost
    - Passing classified information from one company to another in an unauthorized manner or without proper authorization
    - Knowledge of deliberate mishandling of classified information that one fails to report

Topic clarification: The following non-assumptive questions may be used to clarify the security topic for mishandling classified information:

- **Have you ever given classified USG information to a representative of a foreign government?**
- **Have you accepted money or something of value in exchange for giving classified USG information to someone without a USG security clearance?**

- **Have you deliberately handed over classified USG documents to someone who does not possess a USG security clearance?**
- **Have you deliberately passed digitized data media containing classified USG information to someone who does not possess a USG security clearance?**
- **Have you deliberately handed over classified USG equipment to someone who does not possess a USG security clearance?**
- **Have you intentionally discussed in an email any classified USG information with someone who does not possess a USG security clearance?**
- **Have you deliberately removed classified USG information from a secure facility without authorization?**
- **Have you deliberately stored classified USG information in an unauthorized or unsecured location?**
- **Have you provided an unauthorized person with access to a classified USG facility?**
- **Have you provided an unauthorized person with access to classified USG information via any authorized USG computer access?**
- **Has there been any instance when your actions resulted in an unauthorized person gaining access to classified USG information?**

R4: Have you had any unauthorized foreign contacts*?*

Security Concerns: Foreign Influence: 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 coercion by any foreign interest. Adjudication under this Guideline 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 U.S. citizens to obtain protected information and/or is associated with a risk of terrorism.

Conditions that could raise a Security Concern regarding Foreign Influence:

- 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;
- 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;
- Counterintelligence information, that may be classified, indicates that the individual's access to protected information may involve unacceptable risk to national security;

- 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;
- 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;
- Failure to report, when required, association with a foreign national;
- Unauthorized association with a suspected or known agent, associate, or employee of a foreign intelligence service;
- 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;
- Conduct, especially while traveling outside the United States, which may make the individual vulnerable to exploitation, inducement, manipulation, pressure, or coercion;
- Conduct, especially while traveling outside the United States, which may make the individual vulnerable to exploitation, pressure, or coercion by a foreign person, group, government, or country.

Question Definitions:

Unauthorized foreign contact: This is secret, hidden, covert or clandestine contact with a foreign national or a representative of a foreign government, power, group, organization, or firm. A foreign national is a non-US person, however, a representative of a foreign government, power, group or firm can be a US person known to be representing a foreign government or entity. Contact refers to any contact and includes all means of communication (personal, phone, computer, fax, radio or written). This contact would be considered unauthorized if it is covert, hidden, concealed and unreported.

- There are certain countries with which the USG intelligence community has a close working relationship. These countries are Canada, Great Britain, New Zealand and Australia. Many other countries, both friend and foe have demonstrated an intelligence gathering or terrorist threat against the USG.

- As outlined in the definition above, an unauthorized foreign contact can be a US person known to represent a foreign government or entity. Therefore, if the pretest discussion leads to close personal, illegal, professional or business contact with any foreign national obtain the details.

    - Nature of relationship, frequency of contact, type of contact (intimate, casual, professional)
    - Current or past involvement with any foreign government activity, including military.

Note: The term fraternization is defined as recurring unofficial social or business contact, or any type of close personal contact.

- Fraternization does not include sanctioned relationships maintained for operational purposes, routine arms-length commercial transactions for goods or services or unavoidable casual or ad hoc encounters.

- Many foreign countries pose a documented intelligence and or terrorist threat to US citizens and the USG.

    - Many foreign countries are friendly or allied, but still target the USG for intelligence gathering purposes.

Elements: Unauthorized Foreign Contacts:

- Business contact:

    - Own a business in a foreign country.
    - Have foreign nationals as business partners.
    - Own rental property in a foreign country.
    - Have foreign investments.
    - Have foreign bank accounts.
    - Have any type of business relationship with a FIS or FSS.

- Professional contact:

    - Recurring professional contacts with a FIS or FSS that have not been reported.
    - Recurring contact with foreign nationals met at symposiums, conferences or colloquiums that have not been reported.
    - Recurring contact with foreign nationals that are professional in nature such as co-authoring a book or research paper that have not been reported.
    - Sharing information with a foreign national that is official information dealing with examinee's job and has never been reported.

- Illegal or criminal contact:

    - Participating in any illegal act involving a foreign national.
    - Arrested, detained, interrogated or interviewed by foreign law enforcement, FIS or FSS.
    - Assisting any foreign national to illegally enter the US.
    - Personally aware of any foreign national involved in anything illegal or criminal.
    - Knowledge of unauthorized contacts that have been concealed from the USG in consideration of personnel security requirements.
    - Suspicious or repetitive contacts.

- Requests for sensitive or classified information by the contact(s).

- Close personal contact:

  - Routine contact via phone, email, written correspondence.
  - Plans for future contact, even if non-specific in nature.
  - Shared personal affinity or connection including sexual intimacy.
  - Business relationships, to include involvement in illegal activities.
  - Shared living space in U.S. or abroad.
  - This includes overnight stays at examinee's residence by a foreign national.
  - Personal knowledge on the part of a foreign national regarding specific aspect of examinee's job.
  - Any relationship with a foreign national that holds a dual citizenship.
  - Any hidden contact that requires reporting under security regulations.

Topic clarification: The following non-assumptive questions may be used to clarify the security topic for unauthorized foreign contacts:

- **Have you assisted any foreign national with illegal entrance into the U.S.?**
- **Have you assisted any foreign national with illegal immigration into the U.S.?**
- **Have you assisted any foreign national with illegal immigration into any other country?**
- **Have you engaged in any illegal activity with a citizen of a foreign country?**
- **Are you personally aware of any foreign nationals who are engaged in on-going criminal behavior?**
- **Are you personally aware of any foreign national who was previously engaged in any criminal behavior?**
- **Do you have knowledge of unauthorized foreign contacts that have been concealed from the USG for any reason?**
- **Do you have any friends or associates who are citizens of a foreign country?**
- **Have you assisted any foreign national with legal immigration to the US?**
- **Do you know anyone who is a citizen of a foreign country?**
- **Have you purposefully withheld any information about past or current associations with citizens of a foreign country?**

Appendix B
Directed Lie Comparison Questions
Irrelevant Questions
For the TES Format

Directed Lie Comparison Questions (DLC):

The following are the only acceptable directed lies.

All DLC questions must begin "Did you ever...".
"Have you ever" is reserved for the relevant questions

Reference to "specific family members" in a DLC question is not allowed.
This includes spouse, mother, father, brother, etc.

Below are DLC questions authorized at DACA:

Did you ever take any government (*company*) supplies for your personal use?
Did you ever violate a traffic (*fishing, hunting, boating*) law?
Did you ever say something derogatory about another person behind his back?
Did you ever do anything that made a close friend mad at you?
Did you ever say something that you later regretted?
Did you ever lie to a previous supervisor about anything?
Did you ever borrow anything and forget to return it?
Did you ever lie to a co-worker about anything at all?
Did you ever say anything in anger that you later regretted?
Did you ever brag about yourself to impress others?
Did you ever lie to make yourself look important?
Did you ever say anything about someone that was not true?
Did you ever lie to a close friend?
Did you ever commit a minor traffic violation?
Did you ever cheat at golf (*cards, sports, school*)?
Did you ever lose your temper?
Did you ever exaggerate your fishing (*hunting, sports, work*) accomplishments?

Irrelevant questions (I):

The following are the only acceptable irrelevant questions.

Are you now in (state)?
Is today _____?
Do you sometimes drink water?
Are you now on (location)?

Are you sometimes called _____?
Are the lights on?
Are you sitting down?
Are you wearing shoes (sneakers, boots)?
Is this the month of _____?
Is the door closed?

Appendix C
Alternate Relevant Questions

The following are acceptable alternate relevant questions.

When multiple words are provided in parentheses, use only ONE of the words in the actual question.

R-1 Damage to information or defense systems:

- Have you deliberately done something that caused damage to a USG Information Technology System?
- Have you deliberately manipulated *(damaged)* any USG Information Technology System causing it to become a security risk?
- Have you deliberately modified any component of a USG information or defense System causing it damage?
- Have you intentionally performed any action that damaged a USG information or defense system?

Note: The question, "Have you *sabotaged* any US government information or defense systems may be too limited in scope. The term *sabotage* is considered the action of an enemy agent in time of war. The same might be said for using the action verb *destroyed*. To destroy something means that it is completely ruined. An individual could deliberately introduce a malicious code into a computer system that could slow the system down, but not destroy it.

R-2 Espionage or Terrorism:

- Have you committed (*engaged in*) espionage or terrorism against the United States?
- Have you participated in espionage or terrorism against the United States?
- Have you had contact with a FIS or terrorist group?
- Have you had concealed contact with a member of a FIS or terrorist group?
- Have you concealed contact with a representative of a foreign government or a terrorist organization?

R-3 Deliberate mishandling of classified information:

- Have you intentionally mishandled any classified information?
- Have you deliberately failed to properly handle (*protect)* any classified information?
- Have you compromised any classified information?
- Have you compromised any classified material?

Note: The term *mishandle* is broader in scope than compromise. (E.g. Improper packaging classified and placing in the mail may be considered "mishandled" however, the classified

material is not compromised unless an uncleared individual reviews the material). Security violations pertain to the rules and regulations involving the handling, storing, transporting and discussion of classified USG information. All compromises include a security violation, but security violations do not necessarily include a compromise.

R-4 Unauthorized foreign contact:

- Have you ever had any (secret) (hidden) (unreported) (concealed) foreign contacts?
- Are you (concealing) (hiding) any foreign contacts from the U.S. Government?
- Have you ever failed to report any unauthorized foreign contacts?
- Are you concealing contact with any unauthorized foreign national from *(assigned organization)*?

Note: It is important to evaluate your examinee. If examinee is a first generation US citizen or a non-US citizen the polygraph examiner may be considered the foreign national. It is suggested that the term "non-US citizen" might be a better term to use than "foreign national."

If significant information is obtained when discussing the relevant issues, the preferred method is to move to a breakdown test to resolve the issue(s). However, when minor admissions are made the relevant question(s) can be prefaced with an appropriate qualifier:

"Other than what you told me"
"Besides what we have discussed"
"Have you revealed the fullest extent"
"Excluding"

Appendix D

POLYGRAPH EXAMINATION
CONSENT FORM

I, _____, have been asked to undergo a polygraph examination by

_____, regarding NATIONAL SECURITY MATTERS. I understand that:

a. The polygraph examination is voluntary and I must consent in writing prior to undergoing the examination.

b. Adverse action will not be taken against me based solely on a refusal to undergo this examination, and any refusal will not be recorded in my personnel file.

c. Refusal to undergo a polygraph examination does not preclude security investigation by other means.

d. The examiner will provide an explanation of the polygraph instrument and review all test questions prior to each test.

e. The examination area contains the following recording devices:

two-way observation mirror	YES	NO
video recording devices	YES	NO
audio recording devices	YES	NO

f. I understand this examination will be recorded and/or observed.

g. This consent form does not constitute a waiver of my Constitutional rights against self-incrimination.

h. I may consult with legal counsel to answer questions in conjunction with the polygraph examination.

I UNDERSTAND THE PROVISIONS AND FREELY AND VOLUNTARILY CONSENT TO UNDERGO A POLYGRAPH EXAMINATION. NO THREATS HAVE BEEN MADE OR PROMISES EXTENDED TO ME TO OBTAIN MY PARTICIPATION IN THIS EXAMINATION.

DATE	**SIGNATURE OF EXAMINEE**
DATE and TIME	**SIGNATURE OF EXAMINER**
SIGNATURE OF WITNESS	

Appendix E
Transition from first sub-test to the next

1. Inform examinee no obvious issues observed on the test, but it must go through a QC process before a definitive decision can be made.

2. Explain that you are moving to the next sub-test.

3. Next test will have same types of questions - security questions and two types of diagnostic questions.

4. Must be 100% honest on the next set of security questions.

5. Remind examinees it is their responsibility to ask questions if they do not understand something, and to provide thorough and complete information as it relates to the security issues.

6. Also, remind examinees that they will once again be asked some diagnostic questions where they will be asked to lie.

7. The reason – after initial testing some lose the capability of responding because of fatigue and these questions will let you know they have that continued capability of responding when they lie.

Appendix F
TES OUTLINE

The outline is designed to provide a guide for the TES pretest interview. The pretest interview should not be read, memorized and recited as if being read or spoken as if the pretest was a series of bullet statements. The pretest is an elicitation interview seeking reportable information. Once the pretest is concluded the examinee should be fully aware of all the relevant issues and his or her responsibility as it relates to providing complete, straightforward and truthful information regarding those issues.

INTRODUCTION

- Who you are: Name/the polygraph examiner
- Purpose: A security exam to obtain or retain your security clearance/access to a SAP
- Exam consists of several tests
- Will explain all the questions on each test before conducting them

CONSENT (If agency requires it - do rights advisement)

- Read consent form to examinee
- Indicate any recording or observation devices
- Examinee and Examiner sign consent form

OVERVIEW OF PROCEDURES

- Will ask medical and health questions to make sure suitable to take test
- Will explain instrument and how it works
- Will demonstrate how it works – Acquaintance test
- Will discuss all questions prior to each test
- Each test will have security questions and two types of diagnostic questions

RESPONSIBILITY STATEMENT

- **Set the stage**:
  - Different from most job interviews
  - About suitability to possess or retain a TS or access to a SAP
  - *Credibility Assessment* of ability to provide complete and accurate information to security questions on the test

- **Explain the process**
  - Two parts to Credibility Assessment
  - First – discussion of test questions
  - Second – when sensors attached and physiology recorded
  - Must do two things to be successful in this process

- **Fix responsibility** - First
    - Examinee responsibility - If you do not understand something your responsibility to ask questions until you understand.
    - Examiner responsibility – My job is answering all your questions completely so the test will be successful.

- **Encourage truthfulness** – Second – Examinee responsibility
    - Be thorough and accurate when answering the security questions
    - Provide minor detail even if it appears unimportant
    - End of discussion – you should be confident of accuracy of all your statements. If not, then our discussion should continue

- **Seal the deal**
    - Can I count on you to ask me questions if you do not understand something?
    - Can I count on you to be completely straightforward and truthful in all your statements regarding the security questions today?
    - Obtain an affirmative answer

MEDICAL/BIOGRAPHICAL/CM STATEMENT

- Administrative (note-taking)
- Determine medical suitability
- Obtain sufficient biographical information for possible PLC use later
- Do not lay foundation for PLC questions – this is a DLC format
- No lifestyle information discussed – Unless it is brought up by examinee when discussing security questions

COUNTERMEASURES STATEMENT

- Not uncommon to research the topic of polygraph
- Many sites provide bogus information
- Cause many to think they must attempt to influence outcome of polygraph
- Such activity suggests non-cooperativeness and deceptiveness
- Can I count on you not to involve yourself in such activity
- Get affirmative answer

INSTRUMENT AND F3

- Show and explain each component as taught at DACA
- Provide F3
    - Changes result of autonomic system
    - Body produces responses when you lie or conceal information
    - Raised to know right from wrong – can't control changes when you lie
    - Responses are automatic even when the lie is minor
    - Must be 100% honest to the security questions

- Remember your responsibility to ask questions if you do not understand something and be completely honest and thorough when discussing the security questions

ACQUAINTANCE TEST

- Give rationale for the test
  - Become accustomed to the recording components
  - Adjust instrument to your physiology
  - Demonstrate you are capable of responding when you lie
  - Verbally sell upon completion
    - Reacted strongly
    - Must be 100% truthful to security questions

QUESTION REVIEW

- Security questions and two different types of diagnostic questions
- Discuss security questions for the first test
- **Sacrifice Relevant**
  - Need to make sure you are truthful to security issues we are about to discuss so I will ask you:
  - Do you intend to answer the security questions truthfully?

R1 Damage to USG information and defense systems *(Note: This is the topical area. Do not read the question until after the question is scoped)*

- What comes to mind when you think of **damage** to <u>USG information systems</u>?
  - Listen to and evaluate response.
- Short definition: USG information systems are computers and computer systems and everything that links these computers and systems together.
  - The key is the word "damage"
- <u>Unauthorized access</u>
  - Exchange passwords
  - Misuse (porn, private business, piracy)
  - Hacking
- <u>Physical damage</u>
  - Deliberate and intentional
  - Pouring acid or liquid into an information system
  - Breaking hardware, firmware, or components
  - Sabotage
- <u>Uploading a malicious code</u>
  - Purposeful, malicious to do harm
  - Deliberately placing malicious code into USG system
- <u>Unauthorized altering</u>
  - Changing or deleting without proper permission

        - Use of "back doors" or other surreptitious methods to read restricted data
        - Entering someone else's compartmented data without permission
        - Altering a USG computer to accept unauthorized hardware

    - Topic clarification questions (Pick appropriate questions)
        - Have you used a USG computer to transfer classified to any unauthorized person?
        - Have you downloaded classified without proper permission?
        - Have you hacked into a USG computer?
        - Have you intentionally introduced any malicious code?
        - Have you deliberately damaged in any manner?
        - Have you used USG computer to commit a crime?
        - Have you altered info in USG computer without authorization?
        - Have you given your USG computer password to anyone?
        - Are you concealing any unauthorized use of a USG computer?

- What does the topic of <u>damaging USG defense systems</u> suggest to you?
    - Listen to and evaluate examinee's response.
        - <u>Short definition</u>: Refers to military weapon systems used by USG in our nation's defense to include reconnaissance programs. This is equipment associated directly with the security of the US, its military forces, its borders, embassies, and territories.
    - <u>Weapon Systems</u>
        - Orbiting in space; flying in the air; ground based; floating on or under the water
        - Deliberate physical damage or software damage
    - <u>Reconnaissance programs</u>
        - Intentional damage to
        - Intelligence, Surveillance, and Reconnaissance (ISR) programs
        - Can be hand-held, high altitude UAV, manned aircraft or satellites
        - Damage can be physical or uploading malicious code, altering software
    - <u>Computers connecting, controlling or operating</u>
        - Deliberate damage to command and control systems
        - Adding unauthorized software, firmware, or hardware
        - Unauthorized altering of data or deleting data
        - Physical damage
        - Uploading a malicious code
    - <u>Peripheral Equipment</u>
        - Intentional damage
        - For the purpose of slowing down, damaging, or destroying defense systems
    - Topic clarification for damage to USG defense systems (Pick appropriate questions)

- Have you deliberately damaged any USG defense system?
- Have you committed an act of sabotage on any USG property?
- Have you introduced malicious code into a computer connecting defense equipment?
- Have you hacked into a computer to slow down USG defense systems?
- Have you been approached or contacted to engage in sabotage?
- Has any entity not associated with the USG offered you money, training or tasked you to commit an act of sabotage?
- Have you been compensated for any sabotage activity?
- Do you have knowledge of any sabotage activity or planned sabotage activity against the USG?

- Question you will hear on the test – "Have you deliberately damaged any USG information or defense systems"?
  - How would you answer that question?
  - Evaluate the answer.
  - Move to a direct question if withholding behavior is observed.

R2 Involvement in espionage or terrorism against the United States *(Note: This is the topical area. Do not read the question until after the question is scoped)*

- What does the term espionage mean to you?
  - Evaluate answer – Withholding behavior? Ask direct question.

- Definition: Intentional unauthorized release of classified information or material to a foreign government, power, group or organization with intent or reason to believe that such release may be used to injure the USG or provide an advantage to a foreign government, power, group or organization.

- Elements: Unreported personal, professional or business contact with a representative of a FIS or FSS.

- Unreported contact can involve:
  - Approaches or pitches
  - Offering or volunteering
  - Recruitment, training, tasking
  - Improper copying, removing, transporting and storing for espionage purposes
  - Compensation
  - Spotting and assessment activity
  - Unreported knowledge of espionage

- Topic clarification questions: (Pick appropriate questions)

- Have you performed any secret assignment or work for any foreign government?
- Have you accepted money or anything of value from a foreign government?
- Have you had any unreported meetings with a rep from a foreign government?
- Have you had contact with a foreign government by phone? Email? Written correspondence? Third party?
- Have you met anyone you suspect may have been a rep of a foreign government?
- Have you met anyone you suspect may have had official connections with a FIS or FSS?
- Have you been arrested in a foreign country?
- Have you ever been detained in a foreign country?

- What does the word <u>terrorism</u> mean to you?
  - Evaluate examinee's answer – withholding behavior – Ask direct question.

- <u>Definition</u>: Calculated use of violence or threat of violence to induce fear and is intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious or ideological. Terrorist activity can be subversive as it interferes with, undermines, or denies individuals those rights guaranteed under the US Constitution and results in or leads to the violent or illegal attempt to overthrow the USG.

- <u>Elements</u>:
  - <u>Member or previous member</u>
  - <u>Providing support</u> *(time, money, computer or information sharing)*
  - <u>Concealing contact</u>
  - <u>Taking part in or knowledge of</u>

- *Topic clarification questions* (Pick appropriate questions)
  - Are you a terrorist?
  - Have you been a member of any international terror organization such as Al-Qaida or Hezbollah?
  - Have you associated with members of any international terror organization?
  - Have you been a member of a domestic terrorist organization?
  - Have you provided time or money to any domestic terrorist group?
  - Do you know anyone associated with any terrorist group or organization?
  - Have you committed any crime for political or social reasons?
  - Have you assisted others who committed crimes for political or social reasons?
  - Are you withholding any information about your personal connection to terrorist activity?
  - Are you withholding any information about your personal connection with any individual engaged in terrorist activity?

- Question you will hear on the test – "Have you been involved in espionage or terrorism against the United States"?
    - How would you answer that question?

Transition to diagnostic questions:

- Those are the only security issues we will cover on this test.
    - The next sets of questions we will discuss are the diagnostic questions.

Diagnostic Questions:

- Rationale:
    - ACQT demonstrated when you lie you respond.
    - Sometimes people lose the capacity to respond (fatigue, etc.)
    - I need to make sure you maintain the "capability to respond when you lie"
    - Therefore, I am going to ask you some questions to make sure you retain this capability.

- DLC set-up:
    - "We have all at one time or another:
        - Violated a traffic (fishing, boating) law
        - Said something in anger we later regretted
        - Said something derogatory about another behind his back
        - Borrowed something and failed to return it
        - Lost our temper
        - Lied to a close friend
    - Obtain affirmative nod or verbal "yes".
    - Think of a specific instance without telling any detail.
        - When you have a specific instance in mind give an affirmative nod.
    - When I ask you the question – lie to me by answering "no".
    - Review the question to make sure examinees answers "no".
        - After they answer "no", remind them that they are lying about the specific event that they thought of earlier.
        - The answer to the DLC should be as timely as the answers to the irrelevant and relevant questions.
    - Set up the second DLC in the same manner.

- Irrelevant question set-up:
    - Will be asking questions that we both know you are being truthful to when you answer them.
    - I need to see how you respond when telling the truth.
    - Review the irrelevant questions:
        - Are you in the state of _____?

        - Is today _____?
        - Are the lights on?
        - Are you sitting down?
        - Is this the month of _____?
        - Is the door closed?

    - Read the question and obtain an appropriate answer.

Re-review all the questions in this order: SR, R1, R2, C1, C2, I1, I2

- Obtain a verbal answer to each question.
- Make sure examinee answers the DLC questions appropriately.
    - If the answer is inappropriate (e.g. a "yes" answer) provide instructions and ask the question until the examinee gets the answer right.

Prepare examinee for the test:

- Will be asking questions in different order
- Format requires some questions to be asked several times
- Sit still; look ahead, no moving, etc (same procedures as acquaintance test)

Conduct the first sub-test

Evaluate the test data

At DACA, after providing a numeric evaluation to the sub-test check with your instructor before moving to the next phase

If the first sub-test is NSR, transition to the second sub-test:

- Did not see any significant physiology at the security questions, but the results must be validated through a quality control process.

- Will continue with additional testing.
- Next test will have same types of security and diagnostic questions.
- Must be 100% honest on security questions
-. Need to make sure you have the continued capability of responding when you lie.
- Remind examinees of their responsibility to ask questions if they do not understand something and to be thorough in their answers to the security questions.
    - When ready to review DLCs – Explain whether the DLC questions will be the same or different diagnostic questions.
        - If the questions are changed, explain that they were changed in order to help him/her pay attention and answer as reviewed.
            - "Sometimes people become bored, tired or fatigued during testing and fail to pay attention as the test progresses.

- By changing the questions, you will have to pay attention to keep from misanswering the new questions."

Review of security questions for the second sub-test:

- Sacrifice Relevant
  - Need to make sure you are truthful to security issues we are about to discuss so I will ask you:
  - Do you intend to answer the security questions truthfully?

R3 Mishandling classified information *(Note: This is the topical area. Do not read the question until after the question is scoped)*

- What does "mishandling classified information mean to you"?
  - Evaluate answer – Withholding behavior – ask a direct question.

- Definition: Deliberate failure to protect classified information. Removing or storing hard copy, electronic, or memorized classified information with the intent of giving, passing, selling, keeping, or publishing that information for any reason. Includes providing classified or facilitating access to classified information to any unauthorized persons, to include the media, unauthorized US citizens, or foreign nationals. Failing to report efforts by non-cleared individuals to obtain classified information. Unauthorized removal of classified from a secure location and long-term storage outside an approved area. This would include transfer of classified to a non-approved computer.

- Classified refers to USG information only. Three classifications:
  - Confidential
  - Secret
  - Top Secret

- Elements:
  - Providing to an uncleared US citizen or a cleared US citizen without a need-to-know
    - One who does not have a USG security clearance
    - One who has a USG clearance but the information is compartmented and the person does not have a need-to-know
  - Providing to the media or press
    - Radio, TV, Magazines, Newspapers, Book deals
    - Computer blogs, web-sites, bulletin-boards
    - Telephone, FAX, Email, Personal interviews
  - Providing to any foreign national
    - Hidden, conceal or not reported
    - Foreign press or media

        - Foreign embassy, consulate, organization, group
        - US citizen representing a foreign group, organization, government, or country
    - Unauthorized removal and storage
        - Removing from a secure environment to an unsecure or unauthorized environment
        - Placing classified where control is lost
        - Passing to anyone in an unauthorized manner

- *Topic clarification questions for mishandling classified information*(Pick the most appropriate questions)*:*
    - Have you ever given classified USG information to a representative of a foreign government?
    - Have you accepted money or something of values in exchange for giving classified USG information to someone not authorized to receive it?
    - Have you deliberately handed over classified USG information to someone who does not possess a USG security clearance?
    - Have you deliberately passed digitized classified data to someone not authorized to receive it?
    - Have you intentionally discussed in an email any classified USG information with someone who does not possess a USG security clearance?
    - Have you deliberately passed classified information to any member of the media or press?
    - Have you removed classified material from a secure location without authorization?
    - Have you deliberately stored classified material at an unauthorized location?
    - Have you provided an unauthorized person with access to a classified USG facility?
    - Have you provided an unauthorized person with access to classified USG information via any authorized USG computer access?
    - Has there been any instance when your actions resulted in an unauthorized person gaining access to classified USG information?

- Question you will hear on the test – Have you deliberately mishandled any classified information?
    - Obtain the appropriate answer.

R4 Unauthorized foreign contact *(Note: This is the topical area. Do not read the question until after the question is scoped)*

- What does unauthorized foreign contact mean to you?
    - Evaluate examinee's behavior

- Definition: This is secret, hidden, covert or clandestine contact with a foreign national or a representative of a foreign government, power, group, organization or firm. A foreign national is a non-U.S person, however a representative of a foreign government, power, group or firm can be a US person known to be representing a foreign government or entity. Contact refers to any contact and includes all means of communication (personal, phone, computer, fax, radio or written). This contact would be considered unauthorized if it is covert, hidden, concealed and unreported. Such contacts include:

- Elements:
    - Business matters
        - Own a business in a foreign country
        - Have foreign business partners
        - Own rental property in a foreign country
        - Have foreign investments
        - Have foreign bank accounts
        - Have any type of relationship with a FIS or FSS
        - Recurring business contacts of any type with a FN
    - Professional activity
        - Recurring professional contacts with a FIS or FSS
        - Recurring contact with FN met a symposiums, conferences or colloquiums
        - Recurring contact with FN that are professional such as co-authoring a book or research paper
        - Sharing information with a FN that is official information dealing with examinee's job and has never been reported.
    - Illegal behavior, detention, arrest
        - Participating in any illegal act involving a FN
        - Arrest, detained, interrogated or interviewed by foreign law enforcement, FIS or FSS.
        - Assisting any FN to illegally enter the US.
        - Personally aware of any FN involved in anything illegal or criminal.
    - Personal relationships that are close and ongoing
        - Routine contact via phone, email, written correspondence.
        - Plans for future contact, even if non-specific in nature.
        - Shared personal affinity or connection including sexual intimacy.
        - Business relationships, to include involvement in illegal activities.
        - Shared living space in US or abroad.
        - Overnight stays at examinee's residence by a FN.
        - Personal knowledge on part of FN regarding specifics of examinee's job.
        - Any relationship with a FN with dual citizenship.
        - Any hidden contact that requires reporting under security regulations.

- *Topic clarification questions for concealed non-US citizen contact* (Pick appropriate questions)
    - Have you assisted any FN with illegal entrance into the US?
    - Have you assisted any FN with illegal immigration into the US?
    - Have you assisted any FN with illegal immigration into any other country?
    - Have you engaged in any illegal activity with a FN?
    - Are you personally aware of any FN engaged in on-going illegal activity?
    - Are you personally aware of any FN who previously engaged in criminal activity?
    - Do you have any friends or associates who are citizens of a foreign country?
    - Have you assisted any foreign national with legal immigration into the US?
    - Do you know anyone who is a citizen of a foreign country?
    - Have you purposefully withheld any information about past or current associations with citizens of a foreign country?

- Question you will hear on the test – Have you had any unauthorized foreign contacts?
    - Obtain the appropriate answer.

Transition to diagnostic questions:

- Those are the only security issues we will cover on this test.
    - The next questions we will discuss are the diagnostic questions.

Diagnostic Questions:

- Give rationale again (as in previous sub-test)
    - Known lies - to ensure that examinees have continuing capability to respond when they lie
    - Known truth - to see how they respond when they tell the truth

- DLC set-up:
    - "We have all at one time or another:
        - Violated a traffic (fishing, boating) law
        - Said something in anger we later regretted
        - Said something derogator about another behind his back
        - Borrowed something and failed to return it
        - Lost our temper
        - Lied to a close friend
    - Obtain affirmative nod or verbal "yes".
    - Think of a specific instance without telling any detail.
        - When you a specific instance in mind give an affirmative nod.
    - When I ask you the question – lie to me by answering "no".
    - Review the question to make sure examinees answers "no".

        - After they answer "no", remind them that they are lying about the specific event that they thought of earlier.
        - The answer to the DLC should be as timely as the answers to the irrelevant and relevant questions.
    - Set up the second DLC in the same manner.

- Irrelevant question set-up:
    - Will be asking questions that we both know you are being truthful to when you answer them.
    - I need to see how you respond when telling the truth.
    - Review the irrelevant questions:
        - Are you in the state of _____?
        - Is today _____?
        - Are the lights on?
        - Are you sitting down?
        - Is this the month of _____?
        - Is the door closed?
    - Read the question and obtain an appropriate answer.

Re-review all the questions in this order: SR, R3, R4, C1, C2, I1, I2

- Obtain a verbal answer to each question.
- Make sure examinee answers the DLC questions appropriately.
    - If the answer is inappropriate, (e.g. a "yes" answer) provides instructions and ask the question until he or she gets the answer right.

Prepare examinee for the test:

- Will be asking questions in different order
- Format requires some questions to be asked several times
- Sit still; look ahead, no moving, etc (same procedures as acquaintance test)

Conduct the second sub-test

Appendix G

TES SCORE SHEET **Sub-Test __**

First Asking	R__	R__
Pneumos		
Electrodermal		
Cardio		
1st Asking Totals		
Second Asking	R__	R__
Pneumos		
Electrodermal		
Cardio		
2nd Asking Totals		
Third Asking	R__	R__
Pneumos		
Electrodermal		
Cardio		
3rd Asking Totals		
Question Score		

Sub-Test Score	

DECISION	**NSR**	**NO**	**SR**

Examiner_____

Examinee_____

Date and Time_____

Global Review

X – Hit
? – Inc
/ - Acceptable
0 – Artifact

TES A

R1 ___ ___ ___

R2 ___ ___ ___

TES B

R3 ___ ___ ___

R4 ___ ___ ___

Note: Above inserted to assist DACA students in their global review of test data.

Comments: Place on reverse.

Appendix H

FOR OFFICIAL USE ONLY

References

Jayne, Brian C. and Buckley, Joseph P. (2005). *Hiring the Best, Interviewing for Integrity*, John Reid and Associates, Inc.: Chicago, IL.

Krapohl, D. J., and Stern, B.A. (2003). Principles of Multiple-Issue Polygraph Screening: A Model for Applicant, Post-Conviction Offender, and Counterintelligence Testing. *Polygraph*, 32, 201-210.

Meel, P.E., and Rosen, A. (1955). Antecedent probability and the efficiency of psychometric signs, patterns, and cutting scores, *Psychological Bulletin*, 52(3), 194-216.

Recommended Reading

Department of Defense Polygraph Institute Research Division Staff (1995a). *A comparison of psychophysiological detection of deception accuracy rates obtained using the counterintelligence scope polygraph and the test for espionage and sabotage question formats* (DoDPI194-R-0008). Fort McClellan, AL: Department of Defense Polygraph Institute.

Department of Defense Polygraph Institute Research Division Staff (1995b). *Physiological detection of deception accuracy rates obtained using the test for espionage and sabotage* (DoDPI94-R-009). Fort McClellan, AL: Department of Defense Polygraph Institute.

Honts, C.R. (1999). The discussion of questions between test repetitions (charts) is associated with increased test accuracy. *Polygraph*, 28(2), 117-123.

Honts, C. R., and Raskin, D. C., (1988). A field study of the validity of the directed lie control question. *Journal of Police Science and Administration*, 16, 56-61.

Horowitz, S.W., Kircher, J.C., Honts, C.R. and Raskin, D.C. (1997). The role of comparison questions in physiological detection of deception. *Psychophysiology*, 34, 108-115.

Kircher, J.C., Packard, T., Bell, B.G., and Bernhardt, P.C. (2001). *Effects of Prior Demonstrations of Polygraph Accuracy on Outcomes of Probable-Lie and Directed-Lie Polygraph Tests*. Report to the U.S. Department of Defense Polygraph Institute. DoDPI02-R-0002, DTIC AD Number A404128.

Menges, P.M. (2004). Directed lie comparison questions in polygraph examinations. *Polygraph*, 33(3), 131-142.

Milne, R. & Bull, R. (1999). Investigative Interviewing Psychology and Practice, Wiley Series in *The Psychology of Crime, Policing and Law*, (Eds. Davies, G. & Bull, R.). Chichester: John Wiley & Sons, LTD.

Reed, S. (1994). A new psychophysiological detection of deception examination for security screening. *Psychophysiology*, 31, S80 (Abstract).