KLTD Security Solutions, Inc
Initial Security Briefing

Initial Security Briefing - Prior to being granted access to classified information, contractors will provide employees with an initial security briefing that includes:

1. ***Threat Awareness***, including Insider Threat Awareness in according with paragraph (g) in this section
2. ***Counter intelligence (CI) awareness***
3. ***Overview of the information security classification system***.
4. ***Reporting obligations and requirements, including insider threat.***
5. ***Cybersecurity training for all authorized information system*** users in accordance with CSA-provided guidance pursuant to 117.18(a)(1) and (a)(2)
6. ***Security procedures and duties*** applicable to the employee's position requirements (e.g. marking and safeguarding of classified information) and criminal, civil, or administrative consequences that may result from the unauthorized disclosure of classified information, even though the individual has not yet signed an NDA

Security Message

Congratulations!

Your security clearance for access to DoD classified information has been approved. An Initial Security Briefing is required before access may be granted to classified information for all newly cleared personnel (per NISPOM 3-106)
As a Department of Defense (DoD) government contractor, the protection of sensitive government information (both classified and controlled unclassified), is the responsibility
of every employee of KLTD Security Solutions Inc, regardless of how it was obtained or what form it takes.

Our vigilance is imperative in the protection of this information. Anyone with access to these resources has an obligation to protect it. The very nature of our jobs dictate that we lead the way in sound security practices. Anything less is simply not acceptable. This Initial Security Indoctrination provides a good foundation toward that end.

This briefing is designed to ensure you understand and agree to the challenges and responsibilities you will incur upon being granted this privileged access. Please write down any questions you think of while taking this course and be sure to direct them to your Facility Security Officer.

Objective

This briefing will:

- Explain the importance of protecting government assets and what we are protecting
- Provide a basic understanding of DoD security policies
- Identify your personal security responsibilities and reporting requirements

Objective

Discussion topics will include:

- How you got here
  (the request, submission and approval process)
- Personnel Security
  (the Non-Disclosure Agreement, personal reporting requirements, etc.)
- Information Security
  (overview of the classification system; need-to-know principle; identification, handling, and disposal of classified information)
- Physical Security
  (badges, alarms, security procedures, etc.)
- Counterintelligence Awareness
  (threats, reporting obligations and requirements)
- Who to contact for more information

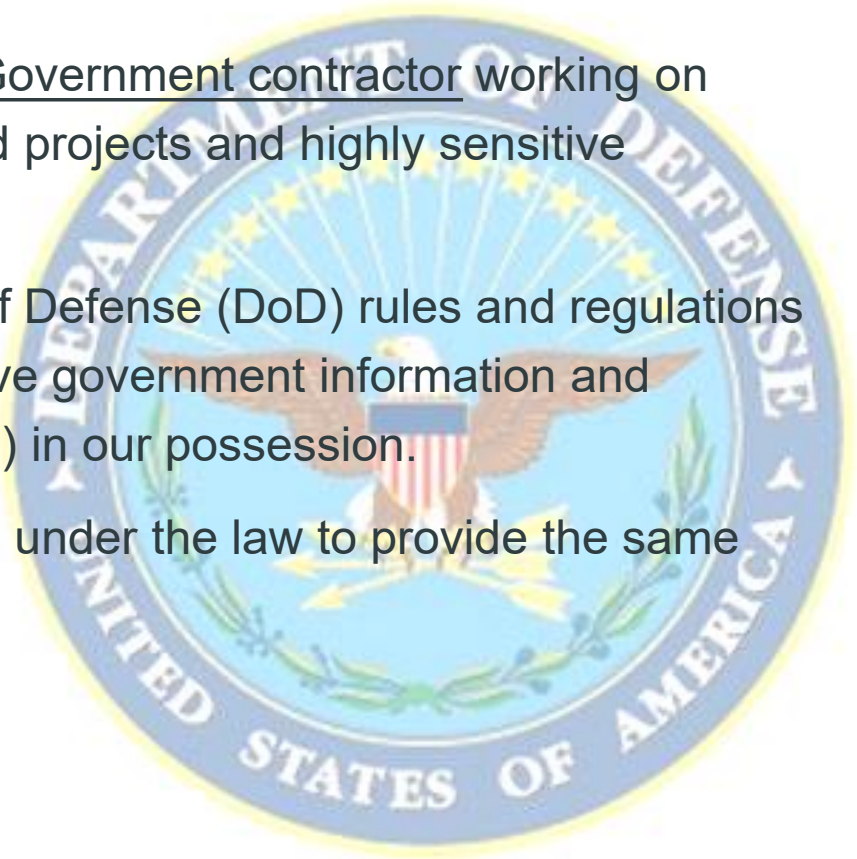
Overview

U.S. Defense Contracting

KLTD Security Solutions, Inc, is a U.S. Government contractor working on contracts that involve specially controlled projects and highly sensitive information.

As such, we are bound by Department of Defense (DoD) rules and regulations to properly protect and control all sensitive government information and material (both classified and unclassified) in our possession.

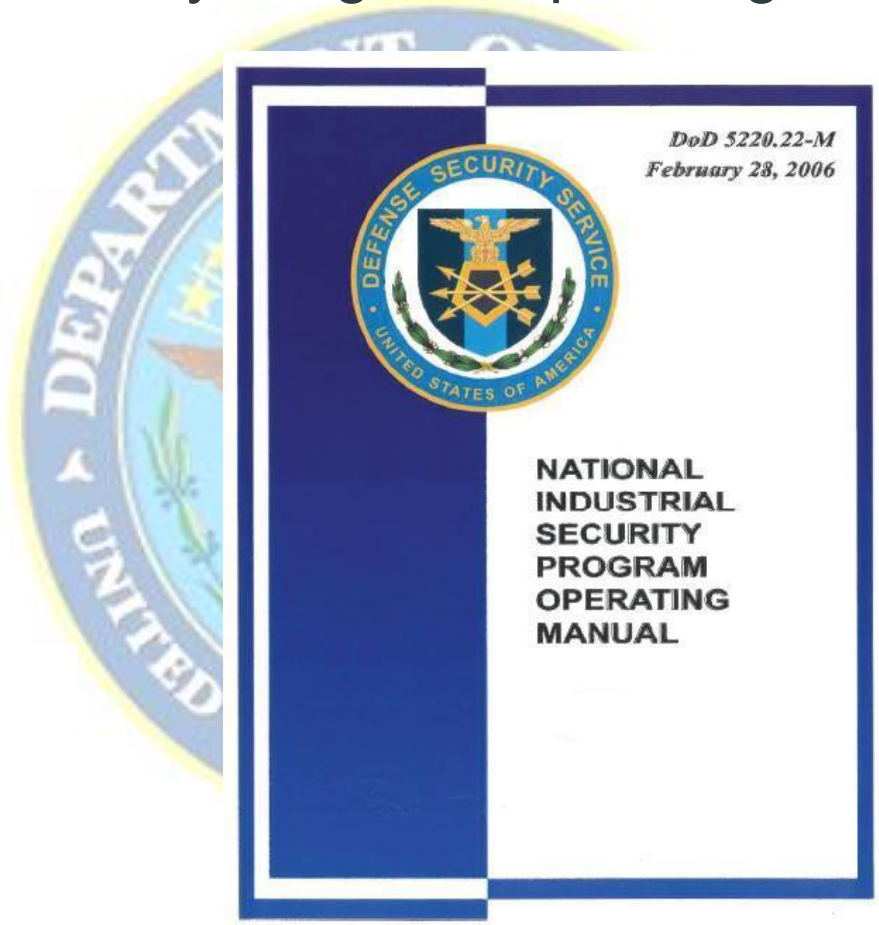
You, as an employee, are equally bound under the law to provide the same protection and control.



Overview

NISPOM: National Industrial Security Program Operating Manual

The NISPOM is the principle document governing U.S. industry in carrying out contracts within the U.S. Government Industrial Security Program KLTD Security Solutions, Inc, is responsible for complying with the requirements of the NISPOM in order to bid on or be awarded a contract involving classified U.S. or foreign government information.



Overview

Why Security?

DoD Security Regulations, Directives, and Programs are established to counter threats to our national security.

Threats to classified and unclassified government assets can include:

- Insider (government employees, contractor employees, and authorized visitors)
- Criminal and Terrorist Activities
- Foreign Intelligence Services
- Foreign Governments

The Government Security Clearance

Why You?

Someone at KLTD Security Solutions, Inc, has determined that they need your expertise in support of one of our classified contracts and, as such, nominated you for access.

You then completed and submitted a personnel security questionnaire disclosing everything about your past history which the government used to complete the required level of Background Investigation (BI) on you.

The type of investigation conducted and level of security clearance you were granted (i.e. Top Secret, Secret, or Confidential) was determined by need based on the sensitivity of your duties.

The Government Security Clearance

Types of Personnel Security Investigations

The Defense Security Service (DSS) – through the Office of Personnel Management (OPM) – conducts several different types of personnel security investigations depending on the type of clearance or access the individual requires. Some of the different types of investigations include:

Single-Scope Background Investigation (SSBI or BI) – the basis for a Top Secret and/or Special Programs access.

National Agency Check, Local Agency Check (NAC/LAC) – the basis for a Secret or a Confidential clearance

Periodic Reinvestigation – the basis for continuing access to information for those previously granted a security clearance:

- Top Secret (required every 5 years)
- Secret (required every 10 years)

Special Investigative Inquiry – conducted when allegations are received about possible unsuitable conduct of a cleared individual

Trustworthiness Investigation – the basis for access to unclassified, but sensitive positions (e.g., individuals who will handle money).

The Government Security Clearance

Adjudicative Standards

Before your security clearance was granted, a specially-trained government adjudicator reviewed your personal history submission and subsequent investigation. The adjudicator then judged and approved you using a "whole person" concept based upon the *13 Adjudicative Standards* listed below. You must continue to conduct your personal life by a high standard in order to maintain your security clearance.

- Allegiance to the United States
- Foreign Influence
- Foreign Preference
- Sexual Behavior
- Personal Conduct
- Financial Considerations
- Alcohol Consumption
- Drug Involvement
- Psychological Conditions
- Criminal Conduct
- Handling Protected Information
- Outside Activities
- Use of Information Technology Systems

If you would like additional information about a particular standard simply click on the title for a description of the standard, the concern and what type of mitigating circumstances may exist. You may then click to return to this slide and to proceed to the next course topic.

Allegiance to the United States

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

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

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

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

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

1) overthrow or influence the government of the United States or any state or local government;
2) prevent Federal, state, or local government personnel from performing their official duties;
3) gain retribution for perceived wrongs caused by the Federal, state, or local government;
4) prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

Conditions that could mitigate security concerns include:

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

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

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

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

Foreign Influence

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

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

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

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

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

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

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

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

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

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

Foreign Influence *(continued)*

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

Conditions that could mitigate security concerns include:

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

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

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

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

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

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

Foreign Preference

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

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

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

1) possession of a current foreign passport;
2) military service or a willingness to bear arms for a foreign country;
3) accepting educational, medical, retirement, social welfare, or other such benefits from a foreign country;
4) residence in a foreign country to meet citizenship requirements;
5) using foreign citizenship to protect financial or business interests in another country;
6) seeking or holding political office in a foreign country;
7) voting in a foreign election;

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

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

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

Foreign Preference *(continued)*

Conditions that could mitigate security concerns include:

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

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

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

d. use of a foreign passport is approved by the cognizant security authority.

e. the passport has been destroyed, surrendered to the cognizant security authority, or otherwise invalidated.

f. the vote in a foreign election was encouraged by the U.S. Government

Sexual Behavior

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

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

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

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

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

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

Conditions that could mitigate security concerns include:

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

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

c.the behavior no longer serves as a basis for coercion, exploitation, or duress.

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

Personal Conduct

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

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

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

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

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

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

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

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

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

1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information:
2) disruptive, violent, or other inappropriate behavior in the workplace;
3) a pattern of dishonesty or rule violations;
4) evidence of significant misuse of Government or other employer's time or resources;

Personal Conduct *(continued)*

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

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

g. association with persons involved in criminal activity.

Conditions that could mitigate security concerns include:

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

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

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

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

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

f. the information was unsubstantiated or from a source of questionable reliability;

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

Financial Considerations

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

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

a.inability or unwillingness to satisfy debts;

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

c.a history of not meeting financial obligations;

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

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

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

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

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

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

Financial Considerations *(continued)*

Conditions that could mitigate security concerns include:

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

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

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

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

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

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

Alcohol Consumption

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

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

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

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

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

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

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

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

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

Alcohol Consumption *(continued)*

Conditions that could mitigate security concerns include:

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

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

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

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

Drug Involvement

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

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

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

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

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

a.any drug abuse (see above definition);

b.testing positive for illegal drug use;

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

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

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

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

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

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

Drug Involvement *(continued)*

Conditions that could mitigate security concerns include:

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

b. a demonstrated intent not to abuse any drugs in the future, such as:
   1) disassociation from drug-using associates and contacts;
   2) changing or avoiding the environment where drugs were used;
   3) an appropriate period of abstinence;
   4) a signed statement of intent with automatic revocation of clearance for any violation;

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

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

Psychological Conditions

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

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

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

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

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

Conditions that could mitigate security concerns include:

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

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

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

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

e.there is no indication of a current problem.

Criminal Conduct

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

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

a.a single serious crime or multiple lesser offenses;

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

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

d.individual is currently on parole or probation;

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

Conditions that could mitigate security concerns include:

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

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

c.evidence that the person did not commit the offense;

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

Handling Protected Information

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

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

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

b.collecting or storing classified or other protected information at home or in any other unauthorized location;

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

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

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

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

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

h.negligence or lax security habits that persist despite counseling by management.

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

Handling Protected Information *(continued)*

Conditions that could mitigate security concerns include:

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

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

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

Outside Activities

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

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

a.any employment or service, whether compensated or volunteer, with:

1) the government of a foreign country;
2) any foreign national, organization, or other entity;
3) a representative of any foreign interest;
4) any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology;

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

Conditions that could mitigate security concerns include:

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

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

Use of Information Technology Systems

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

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

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

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

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

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

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

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

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

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

Conditions that could mitigate security concerns include:

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

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

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

Overview

Security Inspections

Because of KLTD Security Solutions, Inc's, status as a cleared defense contractor we are subject to both scheduled and un-scheduled inspections by various government agencies and higher echelon KLTD Security Solutions, Inc entities to include:

- Defense Security Service
- Various Intelligence Community Agencies
- Department of Justice
- Corporate Security Audit Team
- Other special customers

The purpose of these inspections is to ensure that local security procedures, methods, and physical safeguards are adequate and in compliance with government and/or KLTD Security Solutions, Inc, security regulations.

Most of these inspections include individual employee interviews so it is imperative that you pay particularly close attention to the information contained in this briefing.

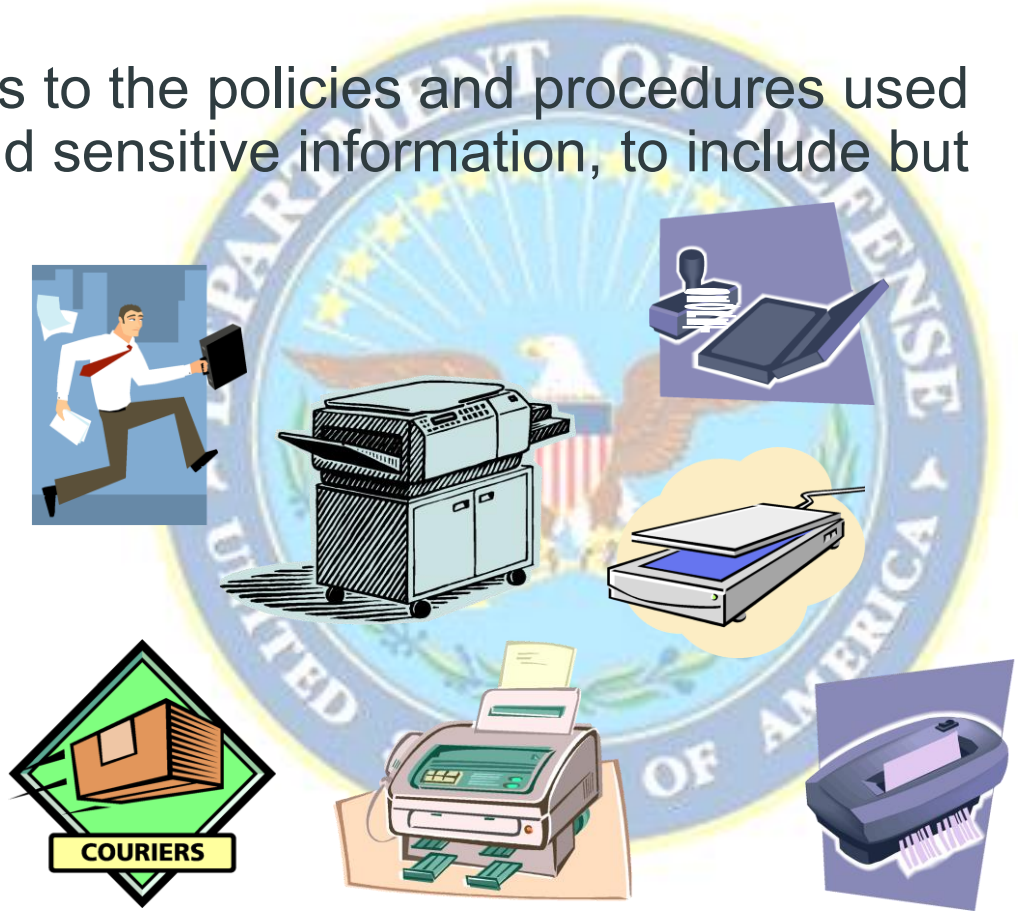
Information Security

Information Security

Definition

Information Security refers to the policies and procedures used to safeguard classified and sensitive information, to include but not limited to:

- Handling
- Marking
- Storage
- Reproduction
- Transmission
- Destruction



Information Security

What Information is to be protected?

Examples of information to be protected includes:

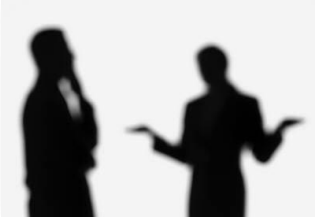
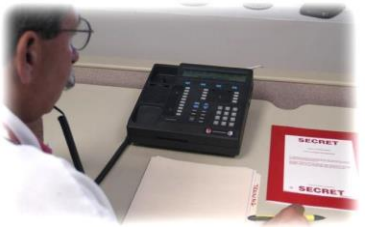
- Government classified information (Top Secret, Secret, & Confidential)
- Government Sensitive But Unclassified (SBU) Information or Controlled Unclassified Information (CUI):
  - (**FOUO**) For Official Use Only
  - (**MCTD**) Military Critical Technology Data
  - (**UCO**) US Citizen Only (more restrictive than US person)
  - (**DCO**) Defense Contractor Only
- Export-controlled information protected under International Traffic in Arms Regulation (ITAR) or Export Administration Regulations (EAR)

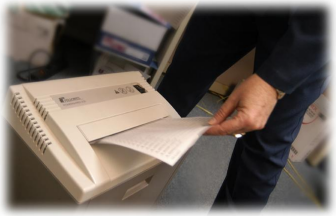
Information Security

Safeguarding Classified Material & Information

Classified information must be…

- Only accessed by individuals with a valid need-to-know
- Under the control or guarded by an authorized person or stored in a locked security container, vault, secure room, or secure area and never be left unattended
- Discussed in an area authorized for classified discussion or on a secure telephone
- Marked appropriately
- Transmitted via secure communications methods
- Processed on computer or other equipment approved by the government
- Destroyed by approved methods

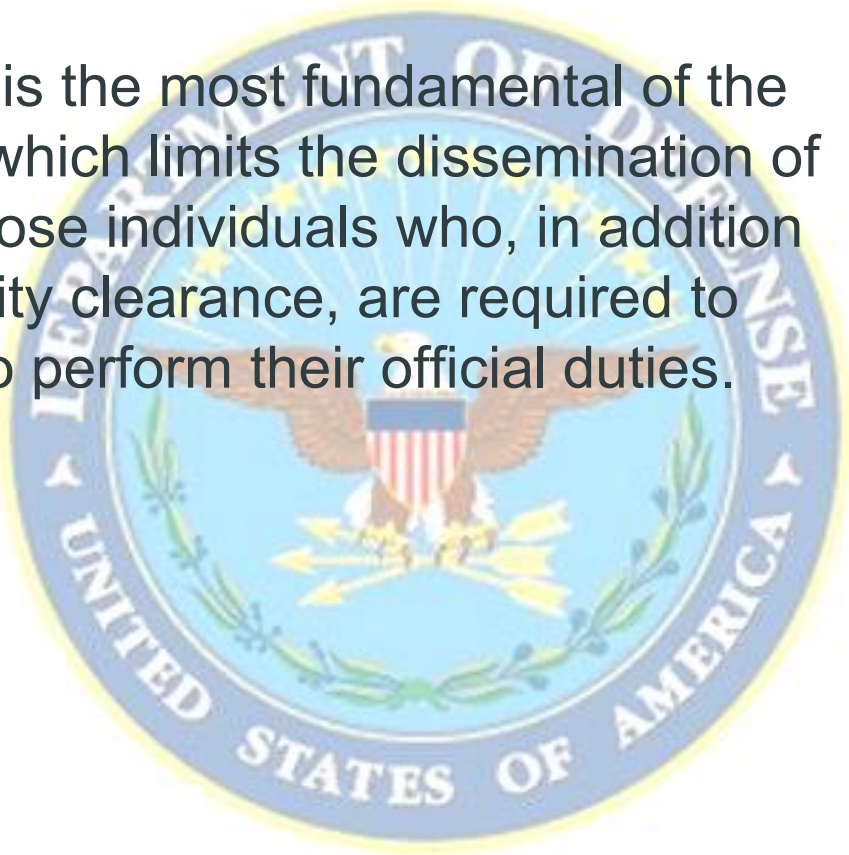




Information Security

Understanding Need-to-Know

The principle of Need-to-Know is the most fundamental of the information security principles which limits the dissemination of classified information only to those individuals who, in addition to possessing the proper security clearance, are required to know the information in order to perform their official duties.



Information Security

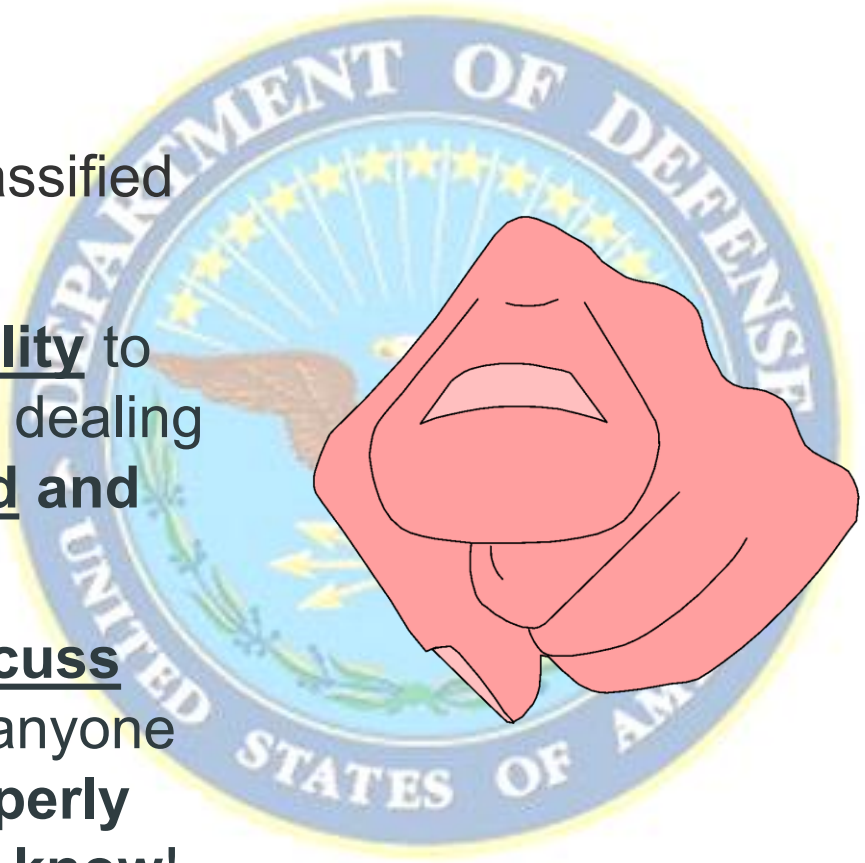
Understanding Need-to-Know

Remember…

You are responsible for any classified item(s) placed in your care!

It is **your personal responsibility** to know that the person you are dealing with is **both properly cleared and has a need-to-know**!

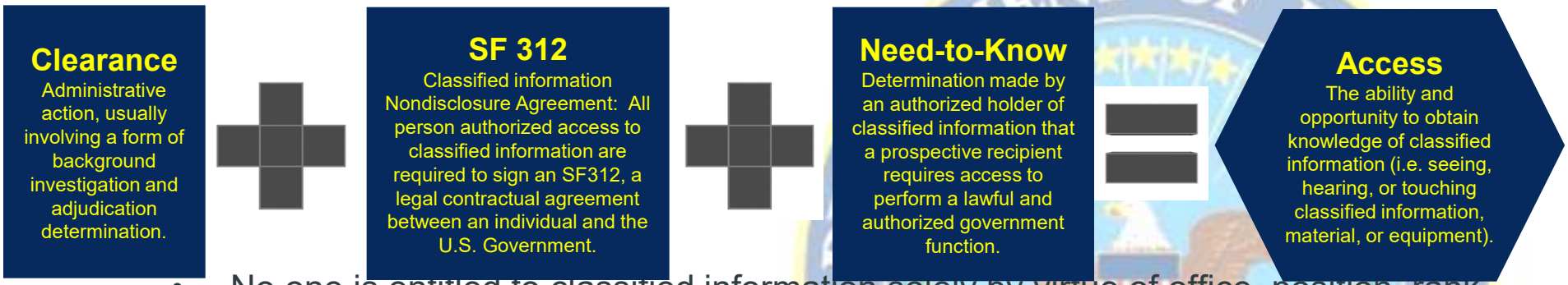
You **must never reveal or discuss classified information** with anyone other than those that are **properly cleared and have a need-to-know**!



Information Security

Access to and Disclosure of Classified Information to Others

Things to remember about Need-to-Know:



- No one is entitled to classified information solely by virtue of office, position, rank or clearance
- You as an authorized holder of classified information have 3 choices in deciding whether or not to share classified material entrusted to you and in your possession:
  1. **Allow access** when all items in the above formula are present
  2. **Deny access** when any item in the above formula is missing
  3. **Delay access** when any of the items in the above formula are unknown.
- Your supervisor or the Program Manager is the best resource for verification of need-to-know.

Information Security

Safeguarding Classified Information

Information Security is all about safeguarding classified and sensitive U.S. Government information. Please click here to view a short video about safeguarding classified information.

Information Security

Safeguarding Classified Information Review

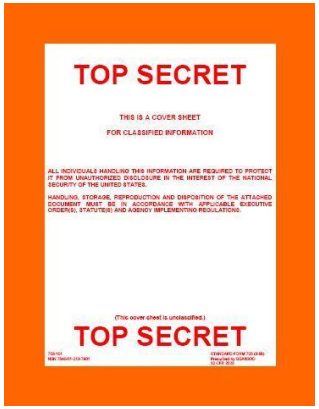
There are THREE distinct levels of classification based on the extent of damage it would cause to our national security if disclosed to persons not authorized to see it.

TOP SECRET

Exceptionally grave damage

Portion marking – (TS)

Coversheet

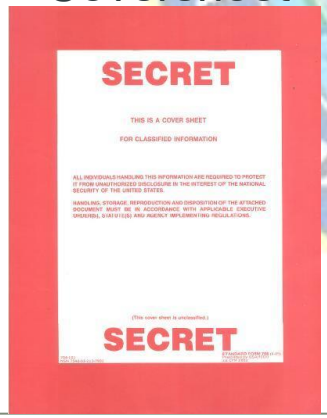


SECRET

Serious damage

Portion marking – (S)

Coversheet

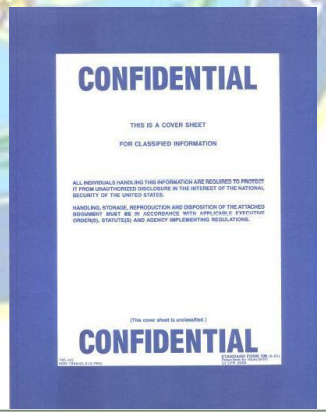


CONFIDENTIAL

Identifiable damage

Portion marking – (C)

Coversheet



Information Security

Safeguarding Classified Information Review

Store classified documents in a GSA-approved storage container when not in use (never store information in a desk, file cabinet, or at home)

- Combinations of GSA approved storage containers are classified at the same level as the highest level of material stored in the container
- Combinations to all DoD containers are safeguarded by the DoD Security Office.
- Commit combinations to memory—DO NOT WRITE THEM DOWN!
- When locking up, spin the combination dial four complete revolutions in one direction and then four more in the opposite direction.

Information Security

Safeguarding Classified Information Review

Information Systems Processing of DoD Classified Information

- Use of personal laptops is PROHIBITED!
- Classified computer processing is allowed on DoD-approved computer systems only.
- Processing DoD classified information on a classified computer network sponsored by one of our other classified customers is allowed **only** if there is a Co-Use/Joint-Use agreement in place with that customer.

Information Security

Safeguarding Classified Information Review

Accountability & Reproduction of Classified Documents:

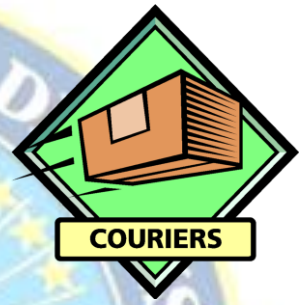
- All original and reproduced DoD classified accountable materials are entered into a control system, tracked, and inventoried regularly.
- All copying of DoD classified documents must be coordinated through the DoD Facility Security Officer
- Printed copies must be kept to the minimum required to meet contractual requirements
- Any reproduced copies shall be marked and protected in the same manner as the original

Information Security

Safeguarding Classified Information Review

Transmission of Classified Documents

- **DO NOT** remove any classified material from a secure area without the knowledge and approval of the Facility Security Officer (FSO).
- All outgoing classified packages must be prepared for transmission by the FSO.
- All incoming packages that may contain DoD classified information (e.g. USPS registered, certified, or Express Mail and FEDEX) are processed by the FSO or other designated receiver before being distributed.
- Classified material removed from the facility must be transported by couriers who have been designated in writing.
  - Get a receipt for the package when you turn it over to another cleared individual.
  - Return the receipt or package to the DoD Security Office upon return.
  - The FSO will check the inventory list
  - No alcohol consumption and/or unnecessary stops while hand-carrying classified info.
- **DO NOT** transmit classified info over a non-secure telephone or fax… coordinate all transfers of classified material through the FSO.



Information Security

Safeguarding Classified Information Review

Electronic Transmission of Classified

If you need to discuss or send classified information via phone or fax, know that…

- All telephone calls may be intercepted (microwave)
- Telephones transmit all background conversations (all!)
- FAX machines by themselves are not secure

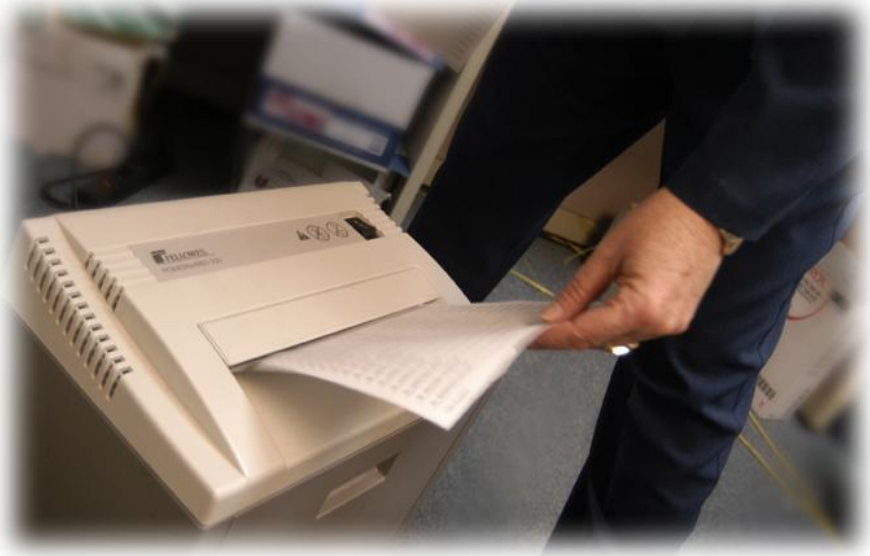
Always use a Secure Terminal Equipment (STE) to conduct classified conversations or a FAX machine that is used in conjunction with a STE to send classified documents.

Information Security

Safeguarding Classified Information Review

Disposition of Classified Material

- Contact the Facility Security Officer in the DoD Security Office for assistance in destroying all DoD classified documents!



Information Security

Marking Classified Documents

All classified material must be marked appropriately in order to:

- Alert the holder of the information that it requires special protection
- Identify the classification level
- Identify why it is classified
- Advise the reader how long it requires protection
- Facilitate downgrading and declassification actions

Information Security

Marking Classified Material Review

Classified material could consist of any of the following:

- Documents
- Working papers
- Emails
- Faxes
- Photographs
- Meeting notes
- Maps & sketches
- Storage media
- Equipment & Machinery
- Other materials

Information Security

Marking Classified Material Review

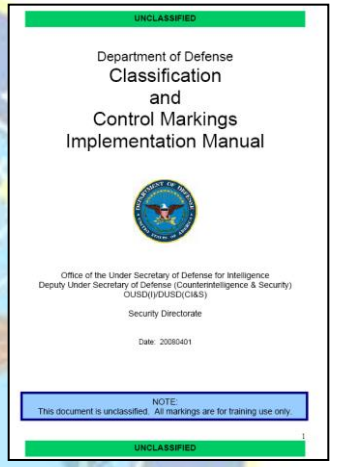
Certain markings are required on every **originally** and **derivatively** classified document. There are not many Original Classification Authorities (OCAs) and they are assigned in writing by the President of the United States.

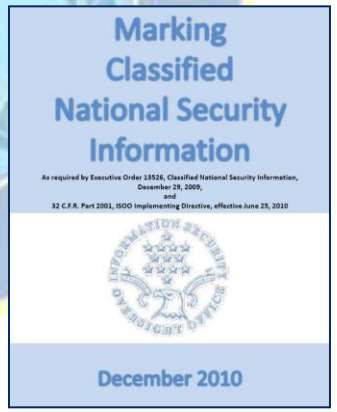
Government industrial companies such as {company name} are only authorized to derivatively classify any documents we create. Required derivative classification markings include:

- Overall classification
- A “Derived from” line for derivatively classified documents
- A “Declassify on” line which indicates when the information is to be declassified
- Portion Markings

Click on the title below or on the picture on the right to view a copy of the:

- DoD Classification & Control Markings Implementation Manual
- ISOO Classification Marking Guide





Information Security

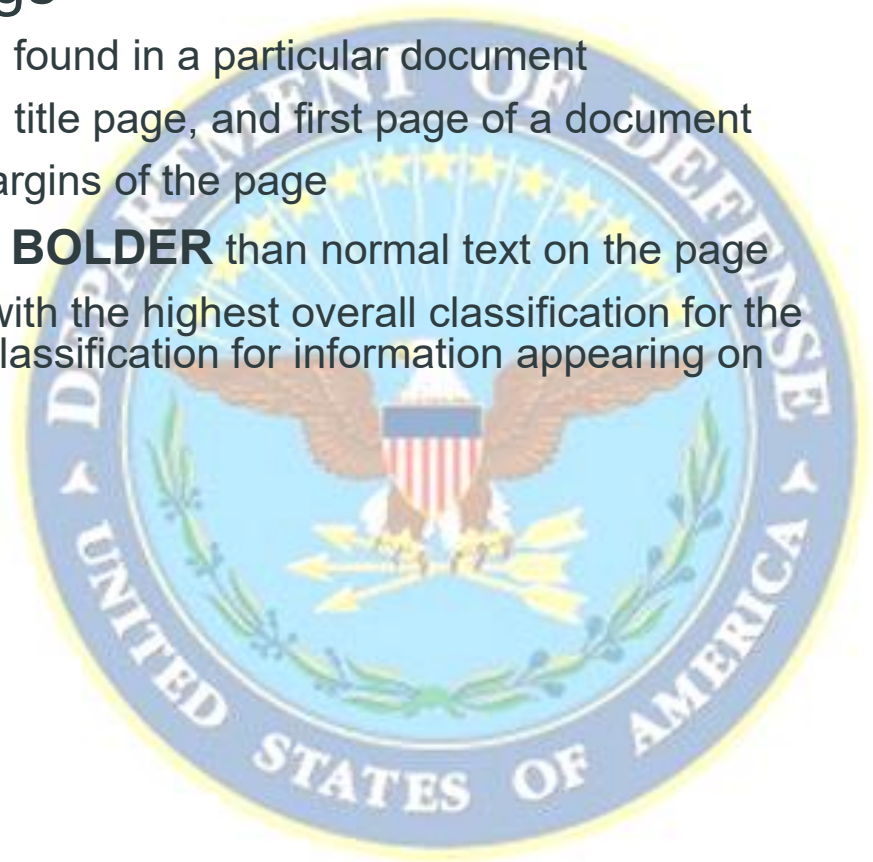
Marking Classified Material Review

Overall Classification Markings

- Reflect the highest level of information found in a particular document
- Are placed on the front & back covers, title page, and first page of a document
- Are centered at the top and bottom margins of the page
- Use a letter font that is LARGER and **BOLDER** than normal text on the page
- Other internal pages may be marked with the highest overall classification for the document **or** with the highest overall classification for information appearing on that page.

Portion Markings

- (TS) for Top Secret
- (S) for Secret
- (C) for Confidential
- (U) for Unclassified



Information Security

Marking Classified Material Review

Requirements for marking and handling Working Papers:

- Labeled as “WORKING PAPERS”
- Marked with overall classification
- Safeguarded in accordance with overall classification
- Dated when created
- Marked with any applicable warning notices
- Cannot be retained for longer than 180 days without becoming a controlled document
- Destroyed when no longer needed
- You are encouraged to use portion markings but ***not*** required to do so (unless they are retained for longer than 180 days)

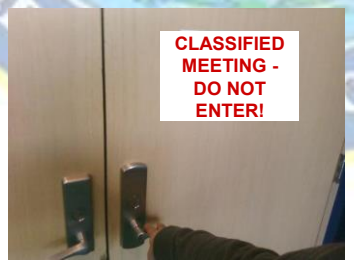
You are responsible for tracking, properly storing, and protecting your working papers!

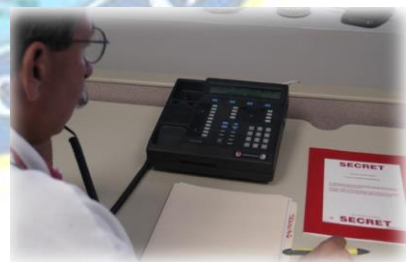
Information Security

Access to Classified Information & Disclosure of Classified Information to Others During Meetings & Discussions

- Classified DoD Contract meetings and discussion must take place in a conference room with a locking device on the door.
- If the room has windows, it must have blinds that can be closed to shield from outside intrusion
- Keep conversations at a low speaking volume so those outside cannot discern what is being said.
- Place a sign on the door stating: “CLASSIFIED MEETING – DO NOT ENTER
- No phone conversations may be conducted except via a secure telephone.





Information Security

Disclosure of Classified Information During Classified Visits

- Before giving a classified document to someone or disclosing classified information orally you must verify the recipient's:
  - Identity
  - Clearance level
  - Need-to-know
- Do not disclose classified information over non-secure commercial telephones or in public places
- Be sure to inform the recipient of the classification level of information disclosed
- Only disclose classified information related to the specific purpose of the visit
- When you are visiting another location, contact the DoD Security Office as soon as possible to pass your clearance information to the cleared facility you will be visiting.

Information Security

Preventing Disclosures of Sensitive Information

Classified information appearing in the media

- At some point in the future you may see information you know to be classified appear in some form in the news media or on the Internet, you **can not** infer that that information has been declassified. If necessary, you may contact the FSO and bring the article or broadcast to our attention (without going into details about the content) so that we may review it and give you a determination on whether you may discuss it and what you can say.
- If you are ever asked by anyone to confirm the authenticity of sensitive information before you are able to talk to the Security Office, you should respond by saying:

"I can neither confirm nor deny any knowledge of that information"

Information Security

Handling Sensitive But Unclassified Material & Information

Information that has not been given a security classification but which is withheld from public disclosure under the criteria of the Freedom of Information Act (FOIA) Title 5, U.S.C. Section 552 such as:

- **(ITAR/EAR)** Export-controlled information protected under International Traffic in Arms Regulation or Export Administration Regulations
- (**FOUO**) For Official Use Only **(NOTE: may NOT be sent via unclassified email)**
- (**MCTD**) Military Critical Technology Data
- (**UCO**) US Citizen Only (more restrictive than US person)
- (**DCO**) Defense Contractor Only

Policy on the storage of Sensitive But Unclassified (SBU) & Controlled Unclassified Information (CUI):

- During working hours: In an out-of-sight location if the work area is accessible to persons who do not have a need for the information
- During non-working hours: Store in a locked desk or cabinet to preclude unauthorized access

Physical Security

Physical Security

Creating “Security-in-Depth”

Physical Security uses a variety of methods, equipment, and procedures to provide “security-in-depth” and includes but is not limited to:

- Perimeter fences
- Employee and visitor access controls
- Intrusion Detection Systems (IDS)
- Random guard patrols & video monitoring
- Prohibited item controls
- Entry/exit inspections
- Escorting
- Employee identification badges

Physical Security

DoD Secure Area Controls

The physical security controls you need to be aware of regarding DoD Labs are:

- Employee and visitor access controls
  - No admittance is allowed to an {your company name} DoD Closed Area unless the employee has a DoD security clearance
  - Uncleared visitors must be escorted by the FSO (or their designee) at all times
  - All visitors must sign the visitor log
  - Incoming visitor clearances may be forwarded via JPAS (SMO Code _____)
- Prohibited items
  - No cell phones
  - No personal electronic devices (without FSO approval)
  - No magnetic media storage devices
  - No recording or photographic devices

Physical Security

Identification Badges

Reef Systems Corp Badge Policy states that your ID badge…

- Must be displayed at all times while on company property
- May only be used by the person whose name and image appear on the front or to whom it is assigned.
- Wear above the waist with picture facing outward
- Report lost badges to Security as soon as possible!

To avoid becoming a target of foreign intelligence officers, we recommend you remove your badge upon exiting the facility.

Physical Security

Standard Employee ID Badges

The KLTD Security Solutions, Inc, Corporate Employee Identification Badge is standardized across all value centers within the corporation and indicates the level of an individual's DoD security clearance (if any).

Company logo indicates bearer is an employee

Colored stripes indicate level of clearance (if any)

Specific value center is listed at the bottom

No U.S. Government DoD Security clearance.

U.S. Government DoD SECRET Security clearance.

U.S. Government DoD TOP SECRET Security clearance.

U.S. Government DoD TOP SECRET security clearance with SCI Access.

Physical Security

Temporary ID Badges

This badge is issued to an Employee on a temporary basis when their picture badge is either lost or forgotten.

Location badge was issued

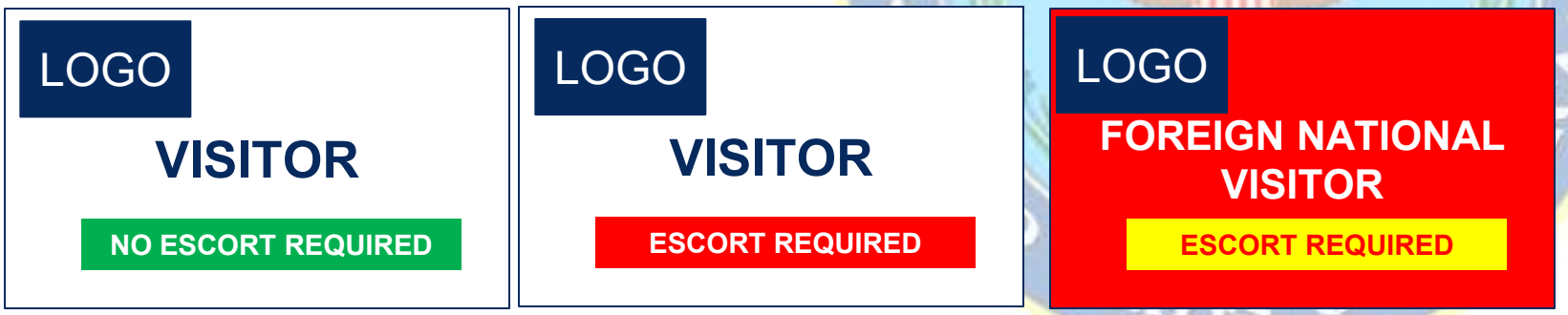
Badge accountability number

Escort requirement (if any)

Physical Security

Temporary ID Badges

The badges below represent the three different types of Visitor badges in use here at Reef Systems Corp:



Physical Security

Identifying Employees with a DoD Security Clearance

The KLTD Security Solutions, Inc, Corporate Employee Identification Badge indicating a DoD security clearance is for identification purposes only and must not be used as the sole means of verification of clearance level and/or “need to know” criteria for accessing classified information.

Personnel Security

Personnel Security

Individual Responsibility

You are responsible for:

- Becoming familiar with local security regulations pertaining to your assigned duties
- Notifying your Security Official of changes in your status which could affect your security clearance.
- Notifying your Security Official and scheduling a debriefing when you leave the company or your duties change such that you no longer need or desire your security clearance and/or access.

Personnel Security

Travel and Visit Clearance Certifications

If you are going to another location and you need your security clearance certification transmitted before your arrival, remember the following:

- Always notify Security about your travel plans *as soon as you know*
- Follow security guidance and provide all requested information to ensure timely transmittal of your visit request.
- Some of the places you visit may take a week or longer to process your visit request (DoE requires at least three weeks to process visit requests).

Personnel Security

Personal Status Reporting Requirements

Change of Personal Status

You must report any changes in your status which could affect your security clearance such as a change of:

- Name
- Marital status
- Citizenship
- Family composition

Examples include:

- Through marriage, you acquire relatives from a foreign country
- You become a representative of a foreign interest by working part time for a company owned by foreign country




Personnel Security

Personal Status Reporting Requirements

Any foreign travel, contacts, or involvements:

- Foreign travel (should be reported as soon as you know but ideally at least 40 days prior to dep[illegible])
- Suspicious or ques[illegible]e or email)
- Any potential employment or service (whether compensated or volunteer) with a foreign individual, organization, government, or other entity or a representative of a foreign interest
- Foreign contacts and ongoing relationships with foreign nationals no matter the method (e.g. meetings/conferences, Internet, e-mail, telephone)
- You must also report contacts with U.S. persons representing a foreign interest—they will not always alert you of this!

The 40-day notice requirement may not be applicable with your government customer.

Personnel Security

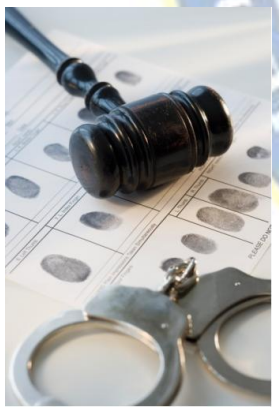
Adverse Information Reporting Requirements

You must also report…

Any adverse information which could make you vulnerable to coercion or exploitation. You must also report these types of information on your coworkers if you become aware of them. Examples include:

- Recent arrests or legal involvement
- Alcohol or drug-related problems





Personnel Security

Adverse Information Reporting Requirements

Also report…

- Financial difficulties or sudden affluence of wealth
- Counseling for emotional, mental or personality disorders
- Sexual behavior indicative of a personality disorder or criminal in nature
- You no longer wish to continue to be processed for a security clearance or continue your access

Counterintelligence Awareness and Additional Reporting Requirements

Counterintelligence/Reporting Requirements

Counterintelligence Awareness – The Threats

As a cleared contractor, you should be aware that you are now a target for foreign intelligence officers. Be wary of and report unsolicited contacts, suspicious activity and other unusual occurrences to your Facility Security Officer.

Some threats include:

- Foreign Intelligence Officers
- Competitors
- Internet
- Hackers
- Faxed requests
- Viruses

Counterintelligence/Reporting Requirements

CI Awareness – Protecting Yourself in an Uncertain World

Unfortunately, just existing in today's world equals exposure to the threat of terrorism. Traveling abroad carries a potentially higher threat level but we are not immune in the U.S. either. When traveling abroad, be cautious about providing information about yourself and your company to those you do not know. The wrong response could place you *in serious jeopardy*. You should:

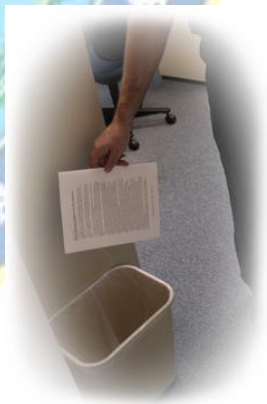
- Plan and prepare well
- Learn about the culture, customs, and laws of countries you visit before departing
- Develop a personal travel plan and give it to your office and family
- Maintain a low profile; don't attract attention to yourself or any official U.S. Government affiliation.

Counterintelligence/Reporting Requirements

Security Violations and Other Occurrences

In addition to the personnel security reporting requirements discussed earlier, you are also required to report any security violations or other threats to national security that you become aware of such as:

- Information about mishandling, loss, compromise, or suspected compromise of classified information
- Classified documents or hardware are left unsecured and unattended (unless in a “Closed Area”)
- A container or Closed Area is left unlocked and unattended

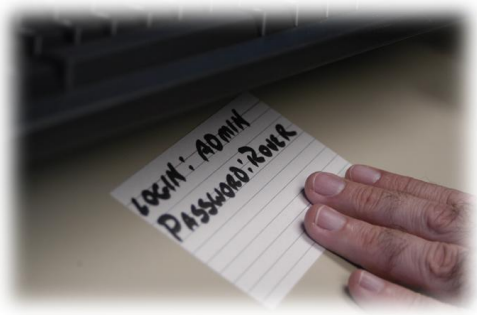


Counterintelligence/Reporting Requirements

Security Violations and Other Occurrences (cont.)

You are also required to report:

- Unauthorized receipt of classified material
- The written combination to a container, vault, strong room, or controlled area is kept in a wallet, purse, desk, etc.
- Classified information is processed, manipulated, or stored on a computer not approved for classified processing

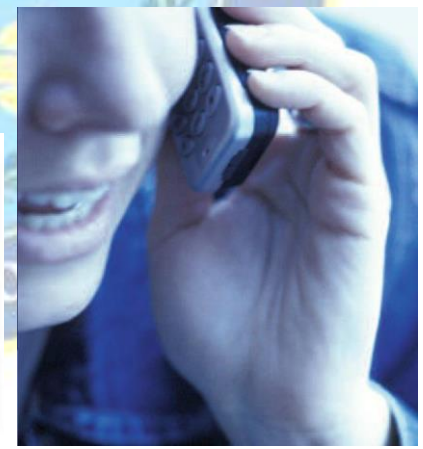


Counterintelligence/Reporting Requirements

Security Violations and Other Occurrences (cont.)

You are also required to report:

- Classified materials hand-carried by a courier are stored overnight in a hotel, car, or other unprotected area
- Classified information is disclosed over an unencrypted (open) telephone or facsimile machine Classified material is released to a subcontractor, vendor, or supplier before the company's facility clearance and safeguarding capability have been verified
- "Bootlegged" copies are made of classified documents



Counterintelligence/Reporting Requirements

Counterintelligence Reporting Requirements

You are also required to report:

- Information about sabotage, espionage, or subversive activities
- Suspicious activities in and around a sensitive area
- An individual is allowed access to a classified document or information or allowed unescorted access to a Secure or Restricted Area without first checking the individual's identity, security clearance and need-to-know.

Counterintelligence/Reporting Requirements

Counterintelligence Awareness – Espionage

The role of the spy, “the Secret Agent”, has become so sensationalized and exaggerated that it is very easy to think that spies exist only in the minds of fiction w

DO NOT BELIEVE IT!

Most of the real life insider spies you see here would have been caught much earlier if fellow employees had reported their bizarre or adverse behavior to supervisors or security.

Do your part and report!

Counterintelligence/Reporting Requirements

Espionage Reporting Requirements

Some of the potential espionage indicators exhibited by others which you must report include:

- Deliberate falsification of security clearance package information
- Attempts to enlist others in illegal or questionable activity
- Inquiry about operations/projects where no legitimate need-to-know exists
- Unauthorized removal of classified information
- Unexplained affluence of wealth or greed
- Divided loyalty or allegiance to the U.S.
- Not associating with fellow employees
- Unreported foreign contact and travel
- Disregarding security procedures
- Keeping unusual work hours
- Verbal or physical threats
- Pattern of lying

Counterintelligence/Reporting Requirements

Espionage Reporting Requirements

You must also report anything that you believe would make an individual susceptible to blackmail or coercion such as:

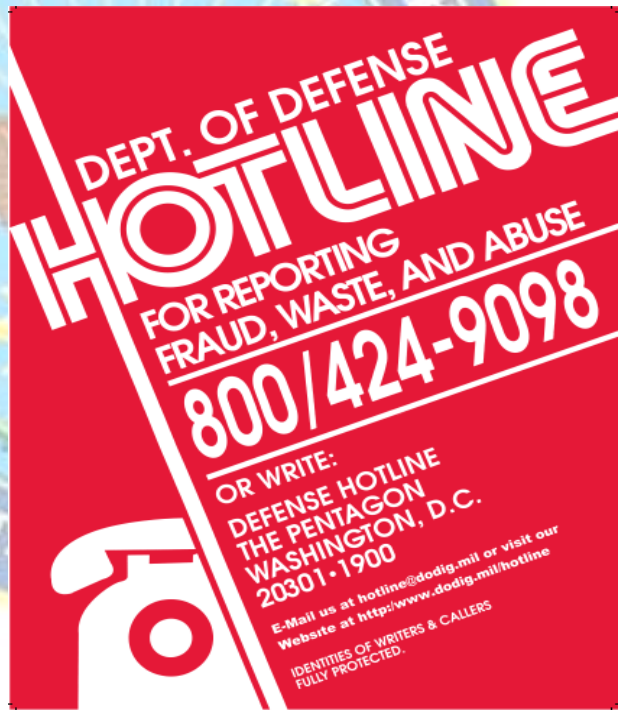
- Excessive debt
- Tampering with IT equipment
- Alcohol or drug use
- Poor judgment in personal conduct
- Unreported security violations

Counterintelligence/Reporting Requirements

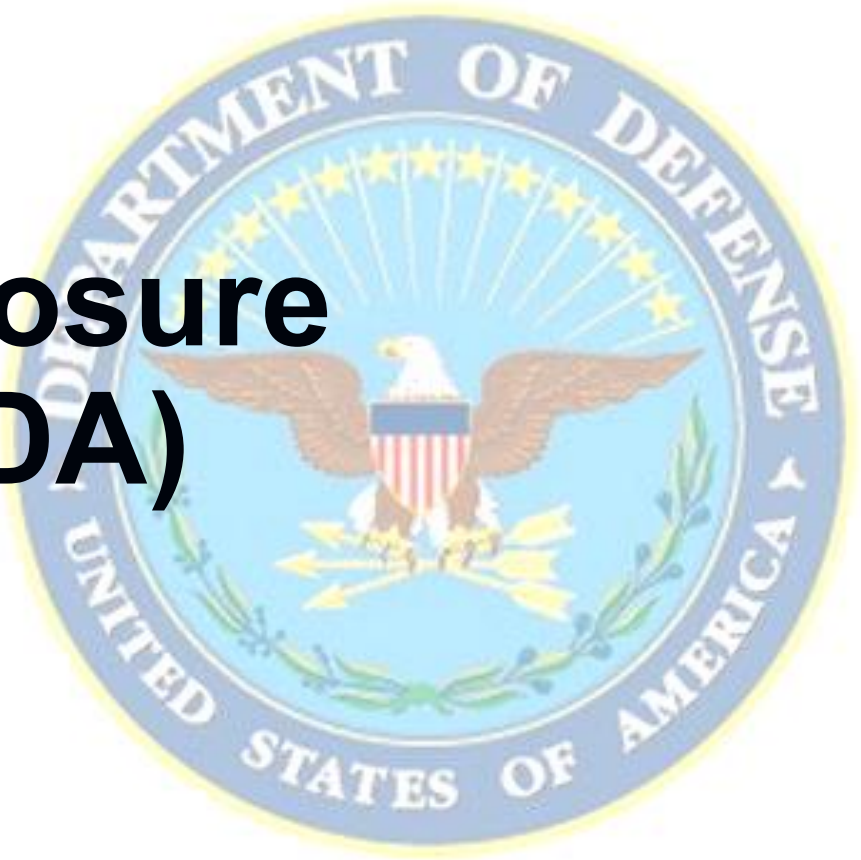
Who to contact

You are also required to report any fraud, waste, or abuse regarding work while working on a government contract.

- You may report concerns either to the FSO or any Security staff member or to the DoD Hotline by phone, email You may report concerns either to the FSO or any Security staff member or to the DoD Hotline by phone, email, or on the web.
- **WARNING:** Do NOT disclose classified information when reporting via one of the DoD Hotline methods as these channels are not secure!
- Other agency hotline numbers (i.e. CIA, NRC, DOE) are listed on page 1-2-2 of the NISPOM
  - These additional hotline numbers do not supplant the normal course of reporting
  - Security encourages employees to report in house as well as to any of the above Hotlines for serious or suspected violations.



The Non-Disclosure Agreement (NDA)



The Non-Disclosure Agreement (NDA)

A Life-Long Commitment!

Before being granted access to classified information, you must first sign a Non-Disclosure Agreement or NDA. The NDA is a **legal** and **binding** contract between you and the U.S. Government whereby you agree to protect any and all classified national security information to which you will have access.

Be advised that the NDA is binding for LIFE!

The Non-Disclosure Agreement (NDA)

Legislative Underpinnings of the NDA

The NDA references several U.S. laws that you will be bound to upon signing it to include the following:

✓Executive Order 12958

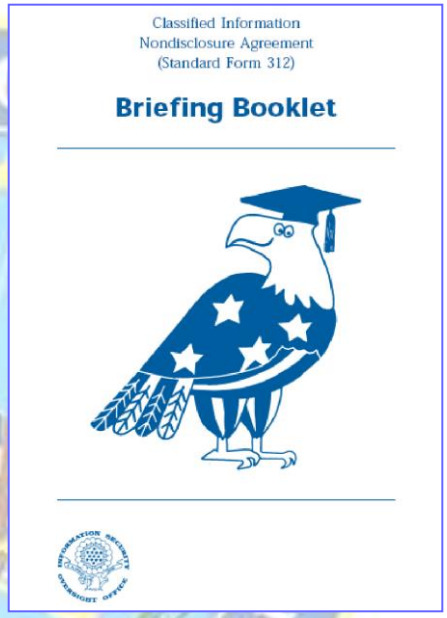
✓Title 18, U.S. Code, Sections 793, 794, 798, 952, 641

✓Title 50, U.S. Code, Sections 783(b), 421

✓Title 5, U.S. Code, Sections 7211, 2302

✓Title 10 U.S. Code, Section 1034

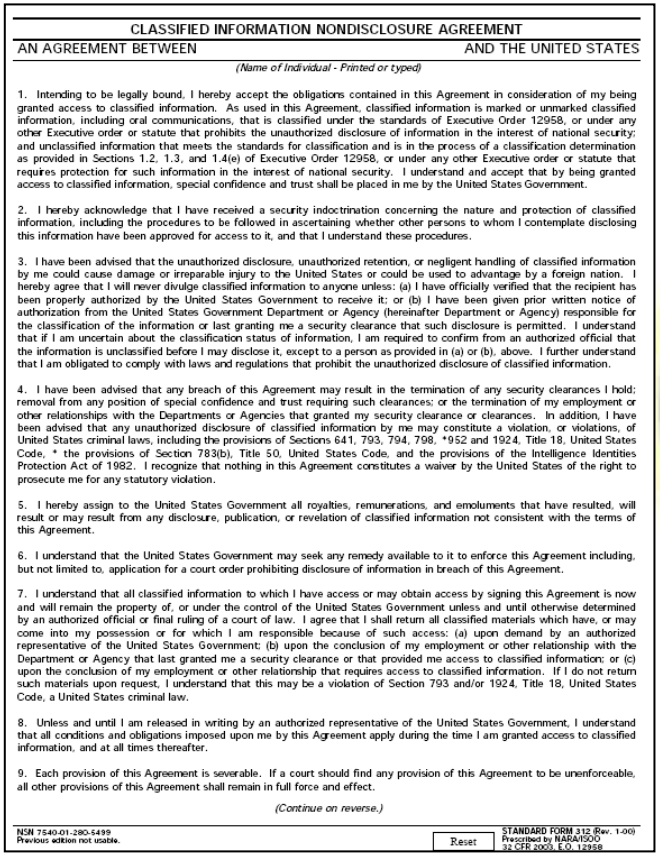
A synopsis of these laws is available for you to review in the NDA briefing booklet you see here. You may click on the picture on the right to view a soft copy of the booklet.



The Non-Disclosure Agreement (NDA)

Standard Form 312

The form you see here is the DoD NDA:



CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.2, 1.3, and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952 and 1924, Title 18, United States Code, * the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable.

Reset

STANDARD FORM 312 (Rev. 1-00)
Prescribed by NARA/ISOO
32 CFR 2003, E.O. 12958

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER *(See Notice below)*

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) *(Type or print)*

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS *(Type or print)*		NAME AND ADDRESS *(Type or print)*	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS *(Type or print)*	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

Reset

STANDARD FORM 312 BACK (Rev. 1-00)

The Non-Disclosure Agreement (NDA)

Standard Form 312 – (In layman's terms)

By signing the NDA, you acknowledge understanding and acceptance that…

Paragraph 1: You are obligated to protect the information that you will be given access to.

Paragraph 2: You received a security briefing concerning the nature of the information you are to be given access to and you understand your responsibilities in protecting it.

Paragraph 3: You can not disclose classified information to someone who is not briefed without specific written authorization to do so.

Paragraph 4: Any breach of this agreement may result in termination of accesses, termination of employment and may constitute a violation of those laws listed in the earlier slide and are available to you for review.

The Non-Disclosure Agreement (NDA)

Standard Form 312 (cont.)

Paragraph 5: You agree to assign to the U.S. Government all rights, titles, and monies that you may receive as a result of any disclosure not consistent with the terms of this agreement.

Paragraph 6: The U.S. Government may seek any remedy available to it to enforce the NDA agreement to include going to court; also if you go to court and you lose, you would pay all court costs including the government's.

Paragraph 7: The information you are being given access to belongs to the U.S. Government and remains the property of the U.S. Government; therefore, you must return all information upon conclusion of your accesses; if you don't you will be violating Section 793 Title 18 U.S. code.

Paragraph 8: You must protect this information **forever** unless given specific written authorization by a cognizant authority to divulge information that was previously classified.

The Non-Disclosure Agreement (NDA)

Standard Form 312 (cont.)

Paragraph 9: Each provision of this agreement stands separate and alone and if a particular paragraph is later deemed unenforceable, it doesn't void the whole agreement—it only voids that one paragraph.

Paragraph 10: The restrictions in this NDA are consistent with and do not supersede or conflict with U.S. law. This NDA agreement is interpreted under and in conformance with the laws of the United States. Also, you are obligated to report any fraud, waste, or abuse that you may encounter while working on a government contract.

Paragraph 11: You have read this agreement at the time of your indoctrination and all your questions were answered and the governing U.S. laws of the NDA were made available to you for review.

The Non-Disclosure Agreement (NDA)

Publication does not equal declassification!

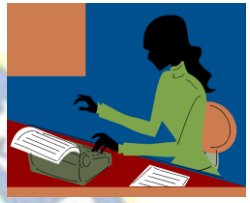
To further clarify paragraph 4 of the NDA, be advised that although at some point in the future you may see information you knew to be classified appear in some form in the news media or on the Internet, you **can not** infer that that information has been declassified. Also, if the existence of a program has actually been declassified, know that our company's involvement in its development may not have been.

If necessary, you may contact KLTD Security and bring the article or broadcast to our attention (without going into details about the content) so that we may review it and give you a determination on whether you may discuss it and what you can say.

The Non-Disclosure Agreement (NDA)

Pre-publication review

If, in the future, you wish to publish anything for public viewing, including resumes, you must first submit it to KLTD Security, FSO Security for a pre-publication review.



Failure to submit items for a security review may subject you to legal proceedings in accordance with paragraphs 3 and 4 of the NDA. Per paragraph 5, you would also have to forfeit any monetary gain received from the unauthorized publication to the government.

Be advised that posting information to the Internet or responding to someone else's post is considered publication!

Cybersecurity Awareness

Cybersecurity awareness is crucial for protecting individuals and organizations from cyber threats, emphasizing the importance of safe online practices and education.

What is Cybersecurity Awareness?

Cybersecurity awareness involves understanding the risks associated with online activities and implementing practices to mitigate those risks. It encompasses recognizing potential threats, such as phishing attacks, malware, and data breaches, and knowing how to respond effectively. This awareness is essential for everyone, from individuals to large organizations, to maintain a secure digital environment.

Importance of Cybersecurity Awareness

1. **Protection Against Cyber Threats**: With the increasing frequency of cyberattacks, being aware of potential threats helps individuals and organizations take proactive measures to protect sensitive information and systems.

2. **Promoting Safe Online Behavior**: Cybersecurity awareness encourages safe practices, such as using strong passwords, enabling multi-factor authentication, and being cautious of unsolicited communications.

3. **Reducing Human Error**: Many cyber incidents result from human error. Educating individuals about cybersecurity can significantly reduce the likelihood of mistakes that lead to security breaches.

Key Actions for Cybersecurity Awareness

- **Use Strong Passwords**: Create long, unique passwords that include a mix of uppercase letters, lowercase letters, numbers, and symbols. Consider using a password manager to help manage and generate strong passwords.
- **Enable Multi-Factor Authentication (MFA)**: MFA adds an extra layer of security by requiring additional verification steps beyond just a password.
- **Be Cautious of Phishing Attempts**: Always verify the source of emails or messages requesting personal information. Avoid clicking on suspicious links or downloading attachments from unknown sources.
- **Educate Others**: Share knowledge about cybersecurity best practices with family, friends, and colleagues to foster a culture of security awareness.
- By prioritizing cybersecurity awareness, individuals and organizations can significantly enhance their defenses against cyber threats and contribute to a safer online environment for everyone.

Conclusion

Information & Guidance

Security Violation Consequences

KLTD Security Solutions, Inc, has a graduated scale of administrative actions that will be taken for failing to adhere to established security rules and regulations.

1st offense: Verbal or written counseling by Security and supervisor

2nd offense: Letter of counseling from Reef Systems Corp company president. Also, Program Manager may at their discretion remove individual from contract work.

3rd offense: Removal from contract

Examples of violations:

- Carrying safe combinations or computer passwords (identifiable as such) on one's person, writing them on calendar pads, keeping them in desk drawers, or otherwise failing to protect the security of a safe or computer.
- Keeping classified material in a desk or unauthorized cabinet, container, or area.
- Failure to follow appropriate procedures for destruction of classified material.

Information & Guidance

Security Awareness, Training & Educations

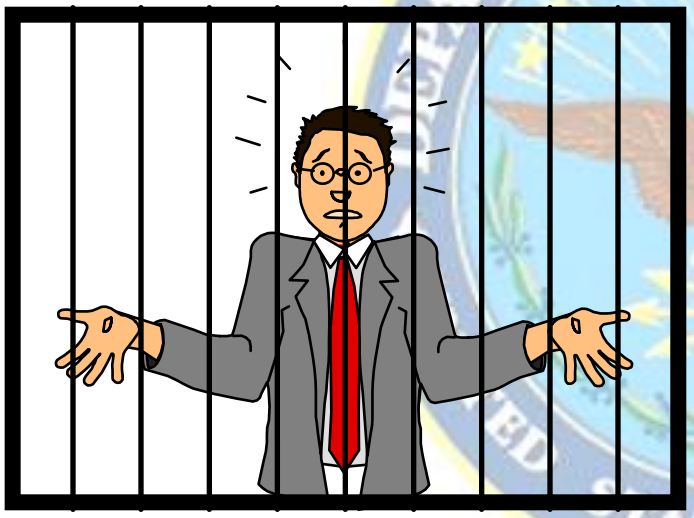
As a cleared employee, you will be required to attend security refresher training on an annual basis and also receive various other security awareness and training information on a recurring basis to include but not limited to:

- Security newsletters
- Memorandums
- Pamphlets
- Periodic bulletins

Information & Guidance

Security Violation Consequences

Be familiar with your security responsibilities! Ignorance does not excuse you from disciplinary or criminal prosecution should an infraction/violation occur.



"All I did was give a friend of mine some information on a competitor's proposal."

Information & Guidance

Security Violation Consequences

Security violations of a blatant and more serious nature including espionage can have even greater consequences including heavy fines and extensive jail time.

Information & Guidance

KLTD Security Solutions, Inc

This facility has been authorized by the Defense Security Service (DSS) to work on classified U.S. government contracts by issuing us a "facility clearance." Below is some basic information regarding our Facility Clearance Listing (FCL):

CAGE (Commercial And Government Entity) Code: 53QF5

SMO Code: 9SBD3 - 1

Facility Clearance Level: None

Storage Level: None

Cognizant Security Office: Virginia Beach Field Office

Assigned Industrial Security Representative: Fenumiai Ilalio, Jr.

Information & Guidance

The final step

This concludes your Initial DoD Indoctrination Briefing. If you agree to the terms and requirements you will be bound to as a condition of being granted this special privileged access, please contact your Facility Security Officer to complete your briefing.

Also, don't forget to bring any questions you may have so that the FSO may address them for you.

DoD Facility Security Officer (FSO)

Information & Guidance

The FSO is the primary point of contact for information and guidance on all DoD security-related matters at a contractor facility.

Your FSO is:

Rad Rouzky
258 Camp Creek Rd
Many, LA 71449
Phone: 502 - 291- 0140
Fax: 928-438-1742
email: Contact@kltdss.com


Security
A
"Personal"
Responsibility