BRIEFING PAPERS® WEST®

SECOND SERIES

PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

DISPUTES INVOLVING ACCESS TO NATIONAL SECURITY INFORMATION

By Thomas M. Abbott and Rob Bohn

Disputes between Government contractors and the Government are sometimes related to the ability to access "classified" information and/or information related to the national security of the United States.[1] These disputes can involve corporate entities or individuals, and their resolution may take place in an administrative proceeding within the agency, before federal administrative law judges, or in federal courts. This BRIEFING PAPER discusses disputes involving a contractor's and/or its employees' ability to obtain access to national security information, as well as the governmental privileges and barriers that apply to the litigation of such disputes.

IN BRIEF

Obtaining Access To National Security Information

■ Contractor Access To National Security Information

Contractors requiring access to national security information must comply with the

Thomas M. Abbott is a partner in the Los Angeles, California office of McKenna Long & Aldridge LLP and Chairman of the firm's Government Contracts practice group. Rob Bohn is an associate in the Government Contracts practice. This BRIEFING PAPER is adapted from a chapter written by Mr. Abbott for GOVERNMENT CONTRACT DISPUTES (Thomson Reuters forthcoming 2010), a treatise prepared by members of the law firm of McKenna Long & Aldridge LLP and by Ronald A. Kienlen, a retired member of the Armed Services Board of Contract Appeals.

requirements of the National Industrial Security Program (NISP), most recently authorized by President Bush in January 1993.[2] The NISP was established to safeguard classified information held by contractors, licensees, and grantees of the U.S. Government and was designed to (1) achieve uniformity in security procedures, (2) apply reciprocity to interagency facility security clearance (FCL) and personnel security clearance (PCL) decisions, (3) eliminate unnecessary or duplicative requirements and inspections, and (4) achieve reductions in overall security costs.[3]

The NISP is implemented by a publication entitled the National Industrial Security Program Operating Manual (NISPOM),[4] and it is administered by the Defense Security Service (DSS) on behalf of the military services, defense agencies, and approximately 23 other federal agencies.[5] The DSS is responsible for the processing, awarding, and monitoring contractors for FCLs. An FCL is an administrative determination that a facility, meaning a company and/or its physical location, is eligible for access to classified information at the same or lower classification category as the clearance being granted.[6] An FCL may be granted at the "Top Secret," "Secret," or "Confidential" level, and a contractor seeking an FCL must execute a Defense Security Agreement in which it agrees to comply with the requirements of the NISPOM.[7] The NISPOM provides the detailed requirements, restrictions, and safeguards that a contractor must implement to prevent the unauthorized disclosure of classified information.[8] In addition, the NISPOM provides guidance on security training and briefings, classification and marking, safeguarding requirements, visits and meetings, subcontracting, information security systems, and international security requirements.

The FCL process starts when a contractor competes for or is awarded a contract that involves the handling of classified information, or when a contractor is sponsored for an FCL by another cleared contractor. To be eligible for an FCL, the contractor must (1) have a valid need to access classified information, (2) be legally organized and existing under the laws of a U.S. state or territory, (3) have a reputation for integrity in its business dealings, (4) not have any of its key managers barred from participating in U.S. Government contracts, and (5) not be under foreign ownership, control, or influence (FOCI) to such a degree that awarding an FCL would be inconsistent with the national interest.[9] The DSS will conduct an initial site inspection of the contractor and require the contractor to identify a senior management official and facility security officer (FSO), both of whom must be processed for clearance (i.e., possess a PCL) to the level of the contractor's desired FCL.[10] The FSO acts as the contractor's chief security officer and "will supervise and direct security measures necessary for implementing applicable requirements of [NISPOM] and related Federal requirements for classified information."[11] In addition, the DSS will work with the contractor to process other officers, directors, and key management personnel for PCLs.

FCL disputes seldom arise at the outset of the FCL application process, and, accordingly, initial FCL denial requests are relatively rare, and the grounds to challenge agency action are extremely limited. Normally, a contractor seeking a first-time FCL has been vetted by the sponsoring, cleared contractor and/or the procuring authority. In the event that a contractor is rejected for an initial FCL application, the contractor has little recourse. Appeals are expressly not authorized for FCL denials based on an overall unsatisfactory security

WEST®

BRIEFING PAPERS

BRIEFING PAPERS® (ISSN 0007-0025) is published monthly except January (two issues) and copyrighted © 2010 ■ Valerie L. Gross, Editor ■ Periodicals postage paid at St. Paul, MN ■ Published by Thomson Reuters / 610 Opperman Drive, P.O. Box 64526 / St. Paul, MN 55164-0526 ■ http://www.west. thomson.com ■ Customer Service: (800) 328-4880 ■ Postmaster: Send address changes to Briefing Papers / PO Box 64526 / St. Paul, MN 55164-0526

evaluation and/or a determination that conditions constitute an immediate danger of compromise to classified information.[12] As discussed below, the courts grant great deference to agency decisions in this arena.

More common are those FCL disputes arising from a contractor's failure to obtain necessary PCLs and/or a failure to exclude representatives of foreign interests. Contractors must report changes in cleared employee status and FOCI information.[13] A contractor with ineligible key management personnel risks suspension and revocation of its FCL unless it takes action to exclude the unqualified individuals.[14] DSS representatives will advise the contractor that the contractor's FCL will be suspended if the contractor fails to take corrective action. The contractor can, under certain circumstances, challenge this demand by seeking review within the DSS. Alternatively, the contractor's board of directors, or similar executive body, must formally resolve that the ineligible parties can be effectively excluded from access to or influence over the organization's policies, practices, or performance of classified contracts.[15] In addition, the excluded parties must make a similar written, and properly recorded, attestation. Procedures for disputing a PCL denial are set forth in detail below.

In addition, a contractor found to be subject to FOCI will be ineligible for an FCL unless it has established security measures to specifically mitigate the FOCI.[16] A company is considered to be under FOCI:[17]

> [W]henever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

In evaluating the extent of the FOCI and the necessary mitigation, the DSS will review the following factors relating to the contractor, the foreign interest, and the government of the foreign interest: (a) the record of economic and government espionage against U.S. targets, (b) the record of enforcement and/or engagement in unauthorized technology transfer, (c) the type and sensitivity of the information to be accessed, (d) the source, nature, and extent of the FOCI, including whether the foreign interests hold a majority or substantial minority position (i.e., an ownership interest greater than 5% or a voting interest greater than 10%), (e) the record of compliance with applicable U.S. laws, regulations, and contracts, (f) the nature of any applicable security and information exchange agreements, and (g) the ownership or control by a foreign government.[18]

FOCI may be addressed through several different mitigating instruments—FOCI action plans—such as board resolutions, voting trust and proxy agreements, and special security agreements and/or security control agreements.[19] These instruments vary in complexity and breadth; however, their overall goal is common—excluding the foreign interest from the ability to access or influence classified information or programs. Careful consideration should be paid to the selection and negotiation of these instruments, and advance coordination and DSS approval is recommended.

■ Contractor Personnel Access To National Security Information

Contractor personnel requiring access to national security information must hold a PCL.[20] The PCL investigation process and initial eligibility determinations are managed by the Defense Industrial Security Clearance Office (DISCO) on behalf of the DSS and are made in accordance with DOD Directive 5200.2-R, "Department of Defense Personnel Security Program," and DOD Directive 5220.6, "Defense Industrial Personnel Security Clearance Review Program." The modern Industrial Security Program and PCL dispute processes were created as a result of the U.S. Supreme Court's 1959 decision in *Greene v. McElroy*.[21] In *Greene,* the Court held that the then-existing security clearance review and appeal processes (determinations by an internal DOD board composed of representatives of the military departments, with no opportunity for cross-examination of witnesses) were unacceptable because neither a statute nor an Executive Order had authorized the program; nor were there discernible standards for denials or revocations.[22] In response to *Greene*, President Eisenhower

signed Executive Order 10865 on February 20, 1960, requiring a hearing at which contractor employees are provided with the opportunity to appear before the decisionmaker to confront and cross-examine witnesses and to attempt to rebut the Government's case.[23]

In *Department of the Navy v. Egan,* the Supreme Court held that individuals do not have a "right" to a security clearance.[24] Rather, "[b]ecause of the extreme sensitivity of security matters, there is a strong presumption against granting a security clearance," and "[w]henever any doubt is raised about an individual's judgment or loyalty, it is deemed best to err on the side of the government's compelling interest in security by denying or revoking a clearance."[25] Accordingly, "a clearance may be granted or retained only if 'clearly consistent with the interests of the national security.'"[26]

To initiate the PCL process, the contractor personnel (the "applicant") must have a valid need to access confidential, secret, or top secret information and must be a U.S. citizen.[27] In rare circumstances, however, a non-U.S. citizen may be granted a limited access authorization.[28] The FSO for the applicant's contractor will initiate a file for the applicant within the Joint Personnel Adjudication System (JPAS) and instruct the applicant to complete Standard Form 86, "Questionnaire for National Security Positions," a fingerprint card, and various authorizations agreeing to the release of personal information to federal investigators. The SF 86 requires extensive information regarding the applicant's citizenship, family members, residential history, educational background, work history, references, foreign contacts, mental and emotional health, police record, drug use, and financial record. Careful attention should be made to the accurate completion of SF 86 as incorrect or misleading answers may be a violation of the criminal false statements statute, 18 U.S.C.A. § 1001, and/or evidence of conduct inconsistent with the honest character required to hold a clearance. There is no meaningful process by which to challenge or dispute the questions on the SF 86, although individuals should not only carefully review the on-line instructions that accompany the on-line application process, they should also not hesitate to ask questions and seek assistance. The overwhelming majority of disputes in this arena are related to incorrect answers to questions on the SF 86.

Once received by the FSO, the applicant's SF 86, fingerprint cards, and releases will make up the applicant's "security clearance package." The FSO will electronically forward this package to DISCO for processing. DISCO will review the applicant's package for completeness and determine if the applicant is eligible for an interim clearance based on the 13 guidelines (Guidelines A through M) contained in DOD Directive 5220.6, Enclosure 2, the "Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information." The DSS website outlines the Adjudicative Guidelines and provides examples of potentially disqualifying conditions:[29]

> 1. Allegiance to the United States. 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.
>
> Example: membership in an organization that supports the overthrowing of the U.S. government.
>
> 2. Foreign influence. A security risk may exist when an individual's immediate family, including cohabitants, and other persons to whom he or she may be bound by affection, influence, or obligation are not citizens of the United States or may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.
>
> Example: foreign financial interest or employment that may affect the individual's security responsibility.
>
> 3. Foreign preference. 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.
>
> Example: possession of a valid foreign passport.
>
> 4. Sexual behavior. Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, may subject the individual to coercion, exploitation, or duress, or reflects lack of judgment or discretion. Sexual

orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.

Example: arrests for a sexual related crime.

5. Personal conduct. Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

Example: subject left previous employment due to fraud.

6. Financial considerations. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

Example: a history of not meeting financial obligations or an inability or unwillingness to satisfy debts.

7. Alcohol consumption. Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness.

Example: treatment for alcohol abuse.

8. Drug involvement. Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

Example: recent drug use, illegal drug possession or drug dependence.

9. Psychological conditions. Emotional, mental and personality disorders can cause a significant deficit in an individual's psychological, social and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability or stability.

Example: information that suggests that an individual has a condition or treatment that may indicate a defect in judgment, reliability or stability.

10. Criminal conduct. A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

Example: felony arrests, multiple misdemeanor arrests or imprisonment for over one year.

11. Handling protected information. Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness and ability to safeguard classified information.

Example: multiple security violations.

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

Example: service or employment country or foreign national.

13. Use of Information Technology Systems. Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

Example: viewing unauthorized web sites.

Interim security clearance awards are to be issued only where facts and circumstances indicate that access to classified information is clearly consistent with the national interest. Moreover, interim awards are unlikely in situations where the applicant's SF 86 indicates disqualifying conditions under one or more of the Adjudicative Guidelines described above.[30]

Upon finding the applicant's package complete, DISCO forwards the package to an "investigative provider," typically, the Office of Personnel Management for investigation. The investigative provider will check national agency records, run a fingerprint check, and verify the applicant's SF 86 information (e.g., the applicant's residential history, academic history, and employment history). The investigator may also contact current and former neighbors, supervisors, co-workers, classmates, and/or references listed on the SF 86. Finally, the investigator may conduct a personal interview of the applicant.[31] Again, the applicant should be aware that his statements made to the investigator are subject to 18 U.S.C.A. § 1001 and that any false or misleading statements may result in an unfavorable eligibility determination.

Once the investigation of the applicant is complete, the case will be assigned to a DISCO "adjudicator" for a determination in accordance with DOD Directive 5220.6 and the Adjudicative Guidelines. The adjudicator will apply the "whole

person" criteria, considering both favorable and unfavorable information in light of the following factors:[32]

(1) the nature, extent and seriousness of the conduct;

(2) the circumstances surrounding the conduct, to include knowledgeable participation;

(3) the frequency and recency of the conduct;

(4) the individual's age and maturity at the time of the conduct;

(5) the extent to which participation is voluntary;

(6) the presence or absence of rehabilitation and other pertinent behavioral changes;

(7) the motivation for the conduct;

(8) the potential for pressure, coercion, exploitation, or duress; and

(9) the likelihood of continuation or recurrence;

Each adjudication is required to be made on its own merits, and any doubt must be resolved in favor of national security.[33] If the DISCO adjudicator cannot affirmatively find that it is clearly consistent with the national interest to grant or continue to grant the applicant a security clearance, DISCO must promptly refer the case to the Defense Office of Hearings and Appeals (DOHA).[34]

■ DOHA Review Of Contractor Personnel Access Decisions

DOHA is primarily responsible for the adjudication, hearings, and appeals of security clearance cases and consists of the director, an appeal board, administrative judges, department counsel, and security specialists. DOHA and its various components are organized under the authority of the General Counsel for the DOD. The administrative judges and department counsel are DOD employees designated by the DOD's Office of General Counsel.[35]

Upon the referral of an applicant's file from DISCO, DOHA will make a prompt determination whether to grant or continue to grant a security clearance.[36] In addition, DOHA may direct further investigation, propound written interrogatories to the applicant, require the applicant to undergo a medical evaluation, and/or interview the applicant.[37] An unfavorable decision must be accompanied by a written statement of reasons (SOR), normally forwarded to the security department of the applicant's employer for hand delivery. The SOR must detail the specific basis for the negative determination and notify the applicant of the applicant's right to submit a timely, written answer and to request a hearing or a decision on the record.[38] The applicant must submit a written, signed, and notarized answer to the SOR within 20 days of receipt. A request for an extension of time may be granted at the discretion of DOHA upon the showing of good cause.[39] The applicant must specifically admit or deny each of the SOR's allegations—a general denial or answer will be found insufficient.[40] An unanswered or insufficiently answered SOR may result in DOHA discontinuing the processing of the applicant's case, denying the requested clearance, and/or revoking any existing clearance.[41] It is highly recommended that applicants request a hearing and appear in person before the DOHA administrative judge. The applicant may appear *pro se* or with counsel,[42] but in either event, the statistics confirm that personal appearances are a significant factor in the successful resolution of these appeals.

In practice, the SOR will specifically allege the Guidelines and associated factual concerns that DOHA believes are inconsistent with awarding the applicant the requested clearance. For example, the SOR will state that DOHA has concerns about the applicant's eligibility under Guideline B, Foreign Contacts, because the applicant's father and brother are citizens and residents of China, and Guideline C, Foreign Preference, because the applicant has a Chinese passport. In answering the SOR, the applicant should specifically admit or deny each allegation as of the date of the applicant's answer. For example, in answering the allegations under Guideline C, Foreign Preference, if the applicant has destroyed or surrendered the applicant's Chinese passport as of the date of the answer, the applicant should deny the allegation. Likewise, if applicant's father or brother have moved or changed citizenship as of the date of the applicant's answer, the applicant should deny those allegations. In addition to the specific denial or admission of the SOR's allegations, the applicant may, but is not required to,

provide additional information in the answer to explain or mitigate the Government's allegations. As a general rule, it is a better practice to provide a simple response to the SOR and present the mitigation or explanation details at the hearing. The applicant may also submit an answer to the SOR with the assistance of counsel and applicant's counsel may make their notice of appearance along with applicant's answer and request that all further correspondence from DOHA be directed to them. Finally, the applicant should state the specific city in which applicant desires a hearing. DOHA will accommodate the applicant's request and generally schedule a hearing near an applicant's place of employment or residence.[43] There are two DOHA hearing facilities: one in Arlington, Virginia, and one in Los Angeles, California. If an applicant is near either of these locations, there may be some advantage in demonstrating a willingness to accommodate DOHA by appearing at one of its facilities.

The submission of applicant's answer to the SOR results in one of three scenarios. First, in very rare instances, DOHA may find that the applicant's answer indicates that the allegations in the SOR are unfounded. In these cases, department counsel (the DOHA attorney assigned to pursue the case on behalf of the Government) will withdraw the SOR and instruct DISCO to award or reinstate the clearance.[44] Second, if neither the applicant's answer nor department counsel has requested a hearing, the case will be assigned to an administrative judge for a determination based upon the record.[45] Under this scenario, department counsel must provide the applicant with a "copy of all relevant and material information that could be adduced at a hearing."[46] The applicant will have 30 days to submit a response and any additional documents.[47] After receiving this response, or after the 30 days have expired and no response has been received, the administrative judge will make a written decision based on the record. The applicant and department counsel will generally have the same appeal rights as those discussed below after a decision based on a live hearing.[48]

Third, if a hearing is requested by the applicant in the answer to the SOR or by department counsel, the case will be assigned to an administrative judge for a decision based upon the hearing record.[49] The hearing must be preceded by at least 15 days' notice.[50] As soon as practical, department counsel and the applicant should exchange any pleadings, documentary evidence, or other written communications they intend to submit to the administrative judge and/or use during the hearing, and the applicant may be entitled to limited discovery.[51] Department counsel has the burden of presenting witnesses and evidence to establish any denied facts alleged in the SOR; however, the applicant has the ultimate burden of persuasion and must establish the application and satisfaction of the mitigating criteria found under the Guidelines at issue.[52] No classified information may be admitted or discussed in the proceedings, which can provide challenges in cases involving allegations of the mishandling of classified information. Both the applicant and department counsel will have the opportunity to cross-examine witnesses, and a written transcript of the hearing will be made and furnished to the applicant without charge.[53] In addition, while the Federal Rules of Evidence serve as a guideline to hearings and appeals, the rules may be relaxed at the discretion of the administrative judge to permit the development of a full and complete record.[54] Finally, the administrative judge may take administrative notice of those facts capable of judicial notice under Federal Rule of Evidence 201.[55] The Federal Rules of Evidence provide for the taking of judicial notice of facts "not subject to reasonable dispute" that are either "generally known within the territorial jurisdiction of the court," or "capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned."[56] Objections to evidence are permitted, and, while the federal rules are relaxed, evidence may be excluded, and its admission over an objection may be grounds for a reversal on appeal.[57]

In practice, department counsel, who will proceed to present the Government's case first at the hearing, can often rely solely on the applicant's admissions in the applicant's answer to the SOR and the documents in the applicant's security clearance investigation file (e.g., SF 86, statements to investigators, FBI criminal report, etc.) to establish a prima facie case of ineligibility—given the high burden on the applicant to

establish that it is clearly consistent with the national interest to grant the applicant a clearance. In such scenarios, department counsel will typically rest upon these documents with the reservation that the applicant take the stand to testify and to submit to cross-examination unlimited to the scope of the applicant's direct examination and/or testimony. It then becomes the applicant's responsibility to specifically mitigate each of the disqualifying conditions listed in the SOR.[58] For example, if the applicant admitted that the applicant's father and brother are citizens and residents of China in the answer to the SOR, then the applicant must mitigate these concerns by proving applicable mitigating conditions. In this instance, the applicant could show that Guideline B, Mitigating Condition (a), applies and has been met by proving that the nature of the relationships with the applicant's father and brother, the nature of the country of China, or the positions or activities of the applicant's father and brother are such that it is unlikely that the applicant will be placed in a position of having to choose between the interests of the applicant's father and brother and the interests of the United States.[59] It is generally recommended that the applicant testify in support of the applicant's case. Witnesses are not placed under oath, but the witnesses are advised that 18 U.S.C.A. § 1001 applies to all statements they make to the administrative judge.[60]

After the conclusion of the hearing and the receipt of the written hearing transcript, the administrative judge will make a written clearance determination specifically setting forth findings of fact, policies, and conclusions as to the allegations in the SOR.[61] A copy of the decision should be issued to both department counsel and the applicant,[62] and either may appeal the determination by filing a notice of appeal with the appeal board within 15 days after the date of the administrative judge's determination.[63] The notice of appeal must be followed by the submission of an appeal brief within 45 days of the date of the administrative judge's decision.[64] (If the appealing party fails to file an appeal brief within the required time period, the administrative judge's decision will become final.[65]) The nonappealing party will then have 20 days to submit an optional reply brief.[66]

Appeal board reviews will be conducted only upon the briefs and the case record below—no new evidence will be reviewed or accepted, and no oral argument is permitted.[67] On appeal, the board addresses the material issues raised by the parties to determine whether there is factual or legal error. There is no presumption of error below; the appealing party must raise claims of error with specificity and identify how the administrative judge committed factual or legal error.[68] Furthermore, there is a rebuttable presumption that an administrative judge considered all the record evidence unless the judge specifically states otherwise.[69] Mere disagreement with the judge's weighing of the record evidence is not sufficient to demonstrate that the judge weighed the evidence in a manner that is arbitrary, capricious, or contrary to law.[70] An administrative judge's decision is not arbitrary or capricious when it considers all relevant factors and all important aspects of the case and offers an explanation that is consistent with the record evidence in the case.[71] Even if an appealing party persuasively argues that a judge made factual or legal errors, it does not necessarily follow that those errors were the result of the judge failing to consider record evidence.[72]

If a party challenges the administrative judge's factual findings, the appeal board must determine whether "[t]he Administrative Judge's findings of fact are supported by such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the same record."[73] The board must consider not only whether there is record evidence supporting a judge's findings, but also whether there is evidence that fairly detracts from the weight of the evidence supporting those findings, and whether the judge's findings reflect a reasonable interpretation of the record evidence as a whole.[74] Moreover, it should be noted that, in practice, an appealing party challenging an administrative judge's credibility determination has a heavy burden on appeal.[75]

If a party challenges a question of law, the appeal board's scope of review is plenary.[76] However, in making a security clearance decision, DOHA is compelled to follow its own regulations.[77]

Finally, even if a party can show that a factual or legal error was committed by the administrative

judge, the appeal board must consider whether the error is harmful or harmless.[78] In making that determination, the appeal board should consider whether the nonappealing party has made a persuasive argument for how the administrative judge's decision can be affirmed on alternate grounds.[79] If the administrative judge's decision cannot be affirmed, the appeal board should consider whether the case should be reversed or remanded.[80]

If an applicant's clearance is revoked or denied as the result of a DOHA hearing, the applicant will be prevented from reapplying for a period of one year after the date of the unfavorable decision.[81] In addition, upon reapplication, the applicant must justify reconsideration to DOHA based upon additional facts that rectify or sufficiently mitigate the original findings.[82]

■ Judicial Review Of Contractor Personnel Access Decisions

In *Department of the Navy v. Egan,* the Supreme Court held that the Merit Systems Protection Board had no authority to review the merits of an executive decision to revoke a security clearance.[83] The Court explained in *Egan* that the normally strong presumption in favor of appellate review of agency decisionmaking "runs aground when it encounters concerns of national security" and that, in this "sensitive and inherently discretionary" area of decisionmaking, the "authority to protect [national security] information falls on the President as head of the Executive Branch and as Commander in Chief."[84] *Egan* was extended by the Court in *Webster v. Doe* to similarly preclude judicial review of the merits of security clearance decisions.[85] These seminal cases have been followed by courts to prevent the judicial review of security clearance decisions, except in very limited circumstances.

However, neither *Egan* nor *Webster* hold as a bright-line rule that federal courts lack the jurisdiction to review the security clearance decisions of the DOD. The cases do, however, hold that individuals do not have a "right" to a security clearance, and, accordingly, "[w]here there is no right, no process is due under the Constitution."[86] What these two decisions do establish is that nonexpert bodies outside the Executive Branch cannot review the *merits* of Executive Branch officials' security clearance decisions.[87] However, courts that have found that they lack jurisdiction to review the *merits* of security clearance decisions have nevertheless concluded that they have jurisdiction to consider two other types of challenges to such decisions: (1) challenges based on the agency's alleged violation of its own regulations and (2) challenges based on the agency's alleged violation of the plaintiff's constitutional rights.

The Supreme Court has held that federal courts have jurisdiction over claims based on an agency's alleged failure to comply with its own regulations.[88] At the same time, courts have generally held that they lack jurisdiction over claims based on violations of an agency's regulations where those claims require, in effect, a review of the *merits* of a security clearance decision.[89] For example, one district court concluded that while it lacked jurisdiction to determine whether the revocation of a petitioner's security clearance was in fact a "commonsense decision" since that would require an evaluation of the merits of the agency's decision, it did have jurisdiction over the petitioner's claims to the extent that the petitioner was asking the court to determine whether the agency entirely *ignored* its obligation—under its own regulations—to make "an overall commonsense decision."[90]

The courts have also indicated that other Constitution-based claims may provide a basis for review of DOHA decisions. *Webster* held that even though § 102(c) of the National Security Act commits security-related Central Intelligence Agency employment decisions to the director's discretion, that statute does not preclude judicial review of constitutional claims.[91] The plaintiff in *Webster* brought a host of such claims, all deriving from his contention that the decision to terminate his CIA employment was related to his homosexuality.[92] The Court held that the district court had jurisdiction over such claims and remanded for further proceedings.[93]

Similar treatment was taken by a court in *Dubbs v. Central Intelligence Agency.*[94] In *Dubbs,* while the court of appeals affirmed the district court's ruling that it had no jurisdiction under the Administrative Procedure Act to review the CIA's denial of a security clearance, it remanded

the matter to the district court to consider the plaintiff's claims that the CIA unconstitutionally discriminated against homosexuals in making security clearance determinations, stating that "a blanket policy of security clearance denials to all persons who engage in homosexual conduct would give rise to a colorable equal protection claim." [95] Finally, in *High Tech Gays v. DISCO*, the court considered a class action lawsuit that challenged a DOD policy of conducting mandatory investigations of all homosexual applicants for security clearances.[96] The plaintiffs alleged that this policy deprived them of their speech and associational rights under the First Amendment and of equal protection of the laws.[97] Without addressing whether the federal courts have jurisdiction to hear these claims, the court ruled in favor of defendants on the merits of the equal protection attack, stating that a challenge to security clearance decisions under the equal protection component of the Fifth Amendment Due Process clause amounts to a colorable constitutional claim.[98]

■ Controlled Access Information

In addition to the procedures for access to classified information, contractors and their personnel performing work for the U.S. Intelligence Community may require access to Sensitive Compartmented Information (SCI) and information protected within other controlled access programs (commonly referred to as "controlled access information"). The Intelligence Community is a coalition of 17 Executive Branch agencies and organizations that work both independently and collaboratively to gather the intelligence necessary to conduct foreign relations and national security activities.[99] In October 2008, the Office of the Director of National Intelligence issued comprehensive Intelligence Community policy reform for access to SCI and controlled access information. Intelligence Community Directive Number 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information" (ICD 704), establishes the overarching guidance for controlled access investigations and determinations. ICD 704 references five associated subparts (Intelligence Community Policy Guidance (ICPG) 704.1 to 704.5) that establish further specific policy guidance for investigative standards and procedures, adjudicative guidelines for determining eligibility, denial and revocation procedures, reciprocity, and a common "Scattered Castles" personnel database.

ICPG 704.2 includes as Annex A the same "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information" as used in DOD Directive 5220.6 (containing disqualifying and mitigating conditions under 13 distinct Guidelines).[100] ICPG 704.3 provides the dispute procedures for the denial or revocation of a controlled access clearance. Under these procedures, a negative determination must be provided by a comprehensive written explanation of the basis for denial, must notify the applicant of the applicant's right to counsel and to request documents, records, or reports underlying the negative determination, and may be reviewable upon a written response and request from applicant.[101] These notifications are typically hand delivered in a letter from an unspecified agency. ICPG 704.3 requires a written response to the applicant's reconsideration request and a written notice of the right to appeal to the head of the applicant's Intelligence Community element. The appeal to the head of the Intelligence Community element may be decided by the element's head himself, in which case the element head's decision will be final, or by a three-member panel.[102] In all cases, the Intelligence Community element may conclusively terminate these appeal procedures if a determination is made that the appeal cannot be conducted "without damaging national security interests."[103]

National Security Privileges

■ Orgins Of The Privileges

The "state secrets" and *Totten* privileges are powerful doctrines of governmental privilege used to prevent the release of information that would pose a danger to the national security of the United States, including its defense capabilities, intelligence-gathering methods, and/or its diplomatic relations

with foreign governments. The two privileges are closely related, but they are distinguishable in their origin and scope. The *Totten* privilege is believed to be rooted in the Constitution and effectively bars an entire claim when the subject matter of the claim itself is secret (e.g., secret contract for clandestine services to the Government).[104] The state secrets privilege is a common-law evidentiary rule, and it bars only the disclosure of classified evidence—the effect of which may (but does not necessarily) preclude the entire claim.[105]

The origins of both doctrines can be first traced back to Aaron Burr's trial for treason in 1807. To aid his defense, Burr sought the production of a letter from General James Wilkinson to President Thomas Jefferson.[106] The Government refused production, asserting that the letter might hold state secrets whose disclosure could jeopardize national security.[107] While the court decided the case on other grounds, it noted in dictum that the defendant's need for the evidence would be weighed against the Government's need for secrecy and that, if the letter contained information that "would be imprudent to disclose, which it is not the wish of the executive to disclose, such matter, if not immediately and essentially applicable to the point, [would], of course, be suppressed."[108] This general principle, that the Government may assert privilege in a court of law over information deemed to be in the interest of national security, has evolved into the *Totten* doctrine and state secrets privilege respectively.

■ Totten Doctrine

The *Totten* doctrine was established by the Supreme Court almost 70 years after the Burr trial in *Totten v. United States*.[109] In *Totten*, the administrator of a former spy's estate sued the U.S. Government claiming that the deceased spy was owed unpaid wages under a secret contract he entered into with President Abraham Lincoln to spy on the South during the Civil War.[110] The Court stated that "[b]oth employer and agent must have understood that the lips of the other were to be forever sealed respecting the relation of either to the matter" and, accordingly, that "[t]he secrecy which such contracts impose precludes any action for their enforcement."[111] The Court dismissed the entire case, saying "[i]t may be stated as a general principle, that public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential."[112]

Totten was reinforced and expanded in *Tenet v. Doe*, where the Court held that the *Totten* doctrine applied to bar all suits "where success depends upon the existence of [claimants'] secret espionage relationship with the Government"—not just those breach of contract claims seeking to enforce the terms of an espionage agreement.[113] In *Tenet*, two former foreign nationals who allegedly spied on their native countries on behalf of the United States during the Cold War filed suit against the CIA claiming estoppel and due process violations stemming from the CIA's alleged failure to provide them with promised financial support. The Court dismissed the spies' claim, holding that the *Totten* rule prohibited suits against the Government based on covert espionage agreements.[114] The Court, moreover, distinguished the *Totten* doctrine from the state secrets privilege and stated that the state secrets privilege and *in camera* reviews "simply cannot provide the absolute protection [the Court] found necessary in enunciating the *Totten* rule."[115]

■ State Secrets Privilege

The state secrets privilege was formally recognized in *United States v. Reynolds*.[116] In *Reynolds*, the widows of three civilians who died in the crash of a B-29 Superfortress aircraft brought suit against the Government and sought production of the U.S. Air Force's official accident investigation reports, as well as statements taken from the three surviving crew members.[117] The Government objected, claiming that the requested material was privileged under Air Force regulations and must be kept secret to protect national security.[118] In addition, the Secretary of the Air Force submitted a letter formally asserting a claim of privilege, stating that "it would not be in the public interest to furnish this report," and the Air Force Judge Advocate General filed an affidavit stating that the "demanded material could not be furnished 'without seriously hampering national security, flying safety and the development of highly technical and secret military equipment.'"[119]

The district court ordered the production of the accident report *in camera* to verify the Government's claims of privilege, and when the Government continued to refuse production, the court found in favor of the plaintiffs on the negligence issue.[120] The court of appeals affirmed and the Supreme Court granted certiorari because the case involved "an important question of the Government's privilege to resist discovery."[121] The Court found in favor of the Government and formally established the state secrets privilege and the prerequisite procedural measures to invoke it, as discussed below.

■ Application Of The State Secrets Privilege

The state secrets privilege belongs to the Government and can only be asserted by the Government—the privilege can neither be claimed nor waived by a private party.[122] To initiate a claim, the head of the department that has control over the secret material must have personally considered the material's privileged nature and must formally file a claim of privilege with the court.[123] This claim must provide enough particularity for the court to make an informed decision as to the nature of the material being withheld and the threat to national security if the material were revealed.[124]

Once the privilege has been properly asserted, the court must first determine whether the information is actually a secret.[125] "[S]imply because a factual statement has been publicly made does not necessarily mean that the facts it relates are true and not a secret."[126] Moreover, the court should only examine "publicly reported information that possesses substantial indicia of reliability and whose verification or substantiation possesses the potential to endanger national security."[127] Further, the court is not limited to considering strictly admissible evidence in determining whether the information is secret.[128] Whenever possible, sensitive information must be disentangled from nonsensitive information; however, courts recognize the limitation in trying to separate the two classifications and, if seemingly safe information is part of a "classified mosaic," "the state secrets privilege may be invoked to bar its disclosure, and the court cannot order the government to disentangle this information from classified information."[129]

Once the court decides that the information is secret, the court will examine whether the claim of privilege is appropriate under the circumstances and "do so without forcing a disclosure of the very thing the privilege is designed to protect."[130] This "evaluation" will be made by applying a balancing test to the respective interests of the parties. In each case, the plaintiff's necessity to access the protected information will determine how far the court must inquire into the details of the privilege and its application. Where there is a strong showing of necessity, the Government's claim of privilege should not be lightly accepted; however, even the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that true state secrets are at stake.[131]

■ Effects Of The State Secrets Privilege

The application of the state secrets privilege can have three effects. First, if the Government properly asserts the privilege over a particular item of evidence, the evidence is completely removed from the case.[132] If the plaintiff cannot then prove the prima facie elements of the claim with nonprivileged evidence, the court may dismiss the claim as it would with any plaintiff who cannot prove their case.[133] Second, if the privilege deprives the *defendant* of information that would otherwise give the defendant a valid defense to the claim, then the court may grant summary judgment to the defendant.[134] Finally, as discussed previously, the *Totten* doctrine will apply to dismiss the plaintiff's entire action, notwithstanding the plaintiff's ability to produce nonprivileged evidence, if the very subject matter of the action is a state secret.[135]

GUIDELINES

These *Guidelines* are intended to assist you in understanding issues related to disputes involving access to national security information by a Government contractor and its employees, as well as the governmental privileges and barriers that apply to the litigation of such disputes. They

are not, however, a substitute for professional representation in any specific situation.

1. Be familiar with the NISPOM, which provides the detailed requirements, restrictions, and safeguards that a contractor must implement to prevent the unauthorized disclosure of classified information.

2. To be eligible for an FCL, a contractor must have a valid need to access classified information, be legally organized and existing under the laws of a U.S. state or territory, have a reputation for integrity in its business dealings, not have any of its key managers barred from participating in U.S. Government contracts, and not be under FOCI to such a degree that awarding an FCL would be inconsistent with the national interest.

3. If a contractor is found to be subject to FOCI, it must implement security measures specifically designed to mitigate the FOCI, such as board resolutions, voting trust and proxy agreements, and special security agreements and/or security control agreements, to be eligible for an FCL.

4. Report all changes in cleared employee status and FOCI information. A contractor with ineligible key management personnel risks suspension and revocation of its FCL unless it takes action to exclude the unqualified individuals.

5. Bear in mind that a contractor rejected for an initial FCL application has little recourse. Appeals are expressly not authorized for FCL denials based on an overall unsatisfactory security evaluation and/or a determination that conditions constitute an immediate danger of compromise to classified information, and the courts grant great deference to agency decisions in this arena.

6. Remember that individuals do not have a "right" to a security clearance. A clearance may be granted or retained only if clearly consistent with the interests of the national security.

7. To be eligible for a PCL, the contractor personnel must have a valid need to access confidential, secret, or top secret information and must be a U.S. citizen. In rare circumstances, a non-U.S. citizen may be granted a limited access authorization.

8. Keep in mind that incorrect or misleading answers on an applicant's SF 86 may be a violation of the criminal false statements statute, 18 U.S.C.A. § 1001, and/or evidence of conduct inconsistent with the honest character required to hold a clearance. Statements made to the investigator handling the security clearance application also are subject to 18 U.S.C.A. § 1001 and any false or misleading statements may result in an unfavorable eligibility determination

9. Applicant's seeking to appeal a denial of a security clearance by DOHA must specifically admit or deny each of the SOR's allegations. An unanswered or insufficiently answered SOR may result in DOHA discontinuing the processing of the applicant's case, denying the requested clearance, and/or revoking any existing clearance. Applicants should request a hearing and appear in person before the DOHA administrative judge.

10. Additional detailed information to explain or mitigate the Government's allegations should be presented at the hearing. Remember that the applicant has the ultimate burden of persuasion and must establish the application and satisfaction of the mitigating criteria found under the Adjudicative Guidelines at issue.

11. Be aware that while the Federal Rules of Evidence serve as a guideline in DOHA hearings and appeals, the rules may be relaxed at the discretion of the administrative judge to permit the development of a full and complete record. Objections to evidence are permitted, and, while the federal rules are relaxed, evidence may be excluded, and its admission over an objection may be grounds for a reversal on appeal.

12. Remember that either department counsel or the applicant may appeal the administrative judge's determination to the DOHA appeal board. Appeal board reviews are conducted only upon the briefs and the case record below. No new evidence will be reviewed or accepted, and there is no oral argument. The appealing party must raise claims of error with specificity and identify how the administrative judge committed factual or legal error.

13. An applicant whose clearance is revoked or denied as the result of a DOHA hearing may not reapply until one year after the date of the unfavorable decision and must justify reconsideration to DOHA based upon additional facts that rectify or sufficiently mitigate the original findings.

14. Recognize that judicial review of security clearance decisions is only available in very limited circumstances. While courts have held that they lack jurisdiction to review the merits of security clearance decisions, they have taken jurisdiction to consider challenges based on the agency's alleged violation of its own regulations and challenges based on the agency's alleged violation of the plaintiff's constitutional rights.

15. Remember that the *Totten* privilege effectively bars an entire claim when the subject matter of the claim itself is secret (e.g., secret contract for clandestine services to the Government), while the state secrets privilege bars only the disclosure of classified evidence— the effect of which may (but does not necessarily) preclude the entire claim. The state secrets privilege can only be asserted by the Government—the privilege can neither be claimed nor waived by a private party.

16. Be cognizant that the ability of a contractor to rely on the state secrets privilege as a defense against third-party claims requires close cooperation with the appropriate federal agency and careful drafting of the rationale presented to the court, which may not be generously received in some courts.

★ REFERENCES ★

1/ See generally Dover, Horan & Overman, "Mergers & Acquisitions—Special Issues When Purchasing Government Contractor Entities," Briefing Papers No. 09-7 (June 2009); West, Lee, Brennan, Wharwood & Speice, "National Security Implications of Foreign Investment in U.S. Government Contractors," Briefing Papers No. 07-11 (Oct. 2007); Burgett & Sturm, "Foreign Nationals in U.S. Technology Programs: Complying With Immigration, Export Control, Industrial Security & Other Requirements," Briefing Papers No. 00-3 (Feb. 2000).

2/ Exec. Order No. 12829, National Industrial Security Program (Jan. 6, 1993), 58 Fed. Reg. 3479 (Jan. 8, 1993).

3/ Exec. Order No. 12829, National Industrial Security Program (Jan. 6, 1993), 58 Fed. Reg. 3479 (Jan. 8, 1993).

4/ DOD Directive 5220.22-M, National Industrial Security Program Operating Manual (Feb. 28, 2006), available at http://www.dss.mil/isp/fac_clear/download_nispom.html.

5/ Including the National Aeronautics and Space Administration, Department of Commerce, General Services Administration, Department of State, Small Business Administration, National Science Foundation, Department of the Treasury, Department of Transportation, Department of the Interior, Department of Agriculture, Department of Labor, Environmental Protection Agency, Department of Justice, Federal Reserve System, Government Accountability Office, U.S. Trade Representative, U.S. International Trade Commission, U.S. Agency for International Development, Nuclear Regulatory Commission, Department of Education, Department of Health and Human Services, Department of Homeland Security, and Federal Communications Commission.

6/ DOD Directive 5220.22-R, Industrial Security Regulation (Dec. 4, 1985).

7/ See DD Form 441, Department of Defense Security Agreement (May 2008).

8/ DOD Directive 5220.22-M ¶ 1-100.

9/ DOD Directive 5220.22-M ¶ 2-102.

10/ DOD Directive 5220.22-M ¶ 2-104.

11/ DOD Directive 5220.22-M ¶ 1-201.

12/ DOD Directive 5220.22-R ¶ C2.1.23.

13/ DOD Directive 5220.22-M ¶ 1-302.

14/ DOD Directive 5220.22-M ¶ 2-106.

15/ DOD Directive 5220.22-M ¶ 2-106.

16/ DOD Directive 5220.22-M ¶ 2-300(c).

17/ DOD Directive 5220.22-M ¶ 2-300(a).

18/ DOD Directive 5220.22-M ¶ 2-301.

19/ DOD Directive 5220.22-M ¶ 2-303.

20/ DOD Directive 5220.22-R ¶ C2.3.

21/ Greene v. McElroy, 360 U.S. 474 (1959).

22/ Greene, 360 U.S. 474.

23/ 25 Fed. Reg. 1583 (Feb. 24, 1960).

24/ Dep't of the Navy v. Egan, 484 U.S. 518, 528 (1988).

25/ Dorfmont v. Brown, 913 F.2d 1399, 1401 (9th Cir. 1990).

26/ Dorfmont, 913 F.2d at 1401 (citing Dep't of the Navy v. Egan, 484 U.S. at 528)

27/ DOD Directive 5220.22-M ¶¶ 2-200(a), 2-209; see http://www.dss.mil/isp/international/laa.html.

28/ DOD Directive 5220.22-M ¶¶ 2-209 to 2-210.

29/ http://www.dss.mil/psco/indus_psc_Intrim.html.

30/ See http://www.dss.mil/psco/indus_psc_Intrim.html.

31/ See http://www.dss.mil/psco/indus_psc_process_applicant.html.

32/ DOD Directive 5220.6, Defense Industrial Personnel Security Clearance Review Program (Jan. 2, 1992), Enclosure 2,

Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information ¶ 2(a) (Aug. 30, 2006).

33/ DOD Directive 5220.6, Enclosure 2, Adjudicative Guidelines ¶ 2(b).

34/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.1.

35/ DOD Directive 5220.6, ¶ 5.2. DOHA also hears appeals from security clearance decisions of some agencies. For example, it hears appeals from the Department of the Navy Central Adjudication Facility (DONCAF) and then makes recommendations to the Navy Personnel Security Appeals Board (PSAB) pursuant to SECNAV M-5510.30 (June 2006).

36/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.2.

37/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.2.

38/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶¶ E3.1.3, E3.1.4.

39/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.4.

40/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.4.

41/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.5.

42/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.8.

43/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.8.

44/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.6.

45/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.7.

46/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.7.

47/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.7.

48/ See DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶¶ E3.1.27, E3.1.28.

49/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.8.

50/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.8.

51/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶¶ E3.1.11, E3.1.13.

52/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶¶ E3.1.14, E3.1.15; see also ISCR Case No. 08-01616, at 2 (App. Bd. July 7, 2009) ("Under [DOD Directive 5220.6], the government presents evidence raising security concerns. Then the burden shifts to Applicant to rebut, explain, extenuate, or mitigate the concerns. The ultimate burden of persuasion to obtain a favorable security clearance decision rests with Applicant.").

53/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance, ¶¶ E3.1.16, E3.1.24.

54/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.19.

55/ "Administrative or official notice is the federal administrative law analogue to judicial notice." ISCR Case No. 02-06478 (App. Bd. Dec. 15, 2003) (citing Zubeda v. Ashcroft, 333 F.3d 463, 479 (3d Cir. 2003); Llana-Castellon v. Immigration & Naturalization Serv., 16 F.3d 1093, 1096 (10th Cir. 1994).

56/ Fed. R. Evid. 201(b).

57/ ISCR Case No. 02-26033 (App. Bd. Mar. 11, 2009).

58/ ISCR Case No. 02-26033 (App. Bd. Mar. 11, 2009) ("After the Government presents evidence raising security concerns, the burden shifts to the applicant to rebut or mitigate those concerns."); see DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.15.

59/ See DOD Directive 5220.6, Enclosure 2, Adjudicative Guidelines ¶ 8(a). Note that "[t]he application of disqualifying and mitigation conditions and whole person factors does not turn simply on a finding that one or more of them apply to the particular facts of a case. Rather, their application requires the exercise of sound discretion in light of the record evidence as a whole." ISCR Case No. 05-03635, at 3 (App. Bd. Dec. 20, 2006).

60/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.18.

61/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.25; see also ISCR Case No. 02-26033, at 2 (App. Bd. Mar. 11, 2009) ("A Judge is required to examine the relevant data and articulate a satisfactory explanation for the decision, including a rational connection between the facts found and the choice made.").

62/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.25.

63/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶¶ E3.1.27, E3.1.28.

64/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.30.

65/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.36.3.

66/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.30.

67/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.29.

68/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶¶ E3.1.30, E3.1.32; see also ISCR Case No. 00-0050 (App. Bd. July 23, 2001).

69/ ISCR Case No. 00-0628 (App. Bd. Feb. 24, 2003).

70/ ISCR Case No. 01-21030 (App. Bd. May 7, 2004).

71/ ISCR Case No. 97-0435 (App. Bd. July 14, 1998) (citing Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983)).

72/ ISCR Case No. 97-0435 (App. Bd. July 14, 1998) (citing Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983)).

73/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.32.1.

74/ ISCR Case No. 02-09892 (App. Bd. July 15, 2004).

75/ ISCR Case No. 02-24254 (App. Bd. June 29, 2004).

76/ DISCR Case No. 87-2107 (Sept. 29, 1992).

77/ Jamil v. Sec'y, Dep't of Defense, 910 F.2d 1203, 1208 (4th Cir. 1990); Duane v. U.S. Dep't of Defense, 275 F.3d 988, 993 (10th Cir. 2002); Nickelson v. United States, 284 F. Supp. 2d 387, 391 (E.D. Va. 2003).

78/ ISCR Case No. 00-0250 (App. Bd. July 11, 2001).

79/ ISCR Case No. 99-0454, at 6 (App. Bd. Oct. 17, 2000) (citing Mass. Mut. Life Ins. Co. v. Ludwig, 426 U.S. 479, 480–81 (1976); Olsen v. Correiro, 189 F.3d 52, 58 n.3 (1st Cir. 1999); United States v. Sandia, 188 F.3d 1215, 1217 (10th Cir. 1999); United

Food & Commercial Workers Union, Local 1099 v. Southwest Ohio Regional Transit Auth., 163 F.3d 341, 349 n.3 (6th Cir. 1998); Swanson v. Leggett & Platt, Inc., 154 F.3d 730, 738 (7th Cir. 1998)).

80/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶¶ E3.1.33.2, E3.1.33.3.

81/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.37.

82/ DOD Directive 5220.6, Enclosure 3, Additional Procedural Guidance ¶ E3.1.38.

83/ Dep't of the Navy v. Egan, 484 U.S. 518 (1988).

84/ Dep't of the Navy v. Egan, 484 U.S. at 527.

85/ Webster v. Doe, 486 U.S. 592 (1988).

86/ Dorfmont v. Brown, 913 F.2d 1399, 1403 (9th Cir. 1990). Note that the due process inquiry may be distinguishable in the case of a clearance for merely "sensitive" information. See Kartseva v. Dep't of State, 37 F.3d 1524 (D.C. Cir. 1994).

87/ Accord Jamil v. Sec'y, Dep't of Defense, 910 F.2d 1203, 1208 (4th Cir. 1990); Hill v. Dep't of Air Force, 844 F.2d 1407, 1411 (10th Cir. 1988); Williams v. Reilly, 743 F. Supp. 168, 171 (S.D.N.Y. 1990).

88/ Webster, 486 U.S. at 602 n.7 (1988) (agency "concede[d]" that federal courts have jurisdiction over claims that agency's security clearance decision violated its own regulations); see also Service v. Dulles, 354 U.S. 363 (1957) (federal courts have power to review an agency's actions to ensure that its own regulations have been followed).

89/ See, e.g., Dorfmont, 913 F.2d at 1402 n.1 (9th Cir. 1990) (court lacked jurisdiction to determine whether DOD had complied with regulation requiring it to determine whether granting security clearance was "clearly consistent with the national interest"); Doe v. Schachter, 804 F. Supp. 53, 62 (N.D. Cal. 1992) (court does have jurisdiction where agency's compliance with its regulations can be determined without reviewing merits of agency's decision).

90/ Chesna v. Dep't of Defense, 822 F. Supp. 90, 95–96 (D. Conn. 1993).

91/ Webster, 486 U.S. at 603.

92/ Webster, 486 U.S. at 601–02.

93/ Webster, 486 U.S. at 603–04.

94/ Dubbs v. Central Intelligence Agency, 866 F.2d 1114 (9th Cir.1989).

95/ Dubbs, 866 F.2d at 1119 n.8 (9th Cir.1989).

96/ High Tech Gays v. DISCO, 895 F.2d 563 (9th Cir.1990).

97/ High Tech Gays, 895 F.2d 563.

98/ High Tech Gays, 895 F.2d at 570.

99/ The member agencies are Air Force Intelligence, Army Intelligence, Central Intelligence Agency, Coast Guard Intelligence, Defense Intelligence Agency, Department of Energy, Department of Homeland Security, Department of State, Department of the Treasury, Drug Enforcement Administration, Federal Bureau of Investigation, Marine Corps Intelligence, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency, Navy Intelligence, Office of the Director of National Intelligence. See http://www.intelligence.gov/about-the-intelligence-community/.

100/ ICPG 704.2, Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information (Oct. 2, 2008).

101/ ICPG 704.3, Denial or Revocation of Access to Sensitive Compartmented Information, Other Controlled Access Program Information, and Appeals Processes 1–2 (Oct. 2, 2008).

102/ ICPG 704.3, at 2.

103/ ICPG 704.3, at 2.

104/ Tenet v. Doe, 544 U.S. 1 (2005).

105/ Tenet, 544 U.S. 1.

106/ United States v. Burr, 25 F. Cas. 30 (C.C.D. Va. 1807) (No. 14692d).

107/ United States v. Burr, 25 F. Cas. at 30–31.

108/ United States v. Burr, 25 F. Cas. at 37.

109/ Totten v. United States, 92 U.S. 105 (1876).

110/ Totten, 92 U.S. at 105–06.

111/ Totten, 92 U.S. at 106–107.

112/ Totten, 92 U.S. at 107.

113/ Tenet v. Doe, 544 U.S. 1, 8 (2005).

114/ Tenet, 544 U.S. at 3.

115/ Tenet, 544 U.S. at 11.

116/ United States v. Reynolds, 345 U.S. 1 (1952).

117/ United States v. Reynolds, 345 U.S. at 2–3.

118/ United States v. Reynolds, 345 U.S. at 3–4.

119/ United States v. Reynolds, 345 U.S. at 4–5.

120/ United States v. Reynolds, 345 U.S. at 5.

121/ United States v. Reynolds, 345 U.S. at 3.

122/ United States v. Reynolds, 345 U.S. at 7.

123/ United States v. Reynolds, 345 U.S. at 7–8.

124/ United States ex rel. Schwartz v. TRW, Inc., 211 F.R.D. 388, 394 (C.D. Cal. 2002).

125/ Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 986 (N.D. Cal. 2006).

126/ Hepting , 439 F. Supp. 2d at 990.

127/ Hepting, 439 F. Supp. 2d at 990.

128/ Hepting, 439 F. Supp. 2d at 991.

129/ Kasza v. Browner, 133 F.3d 1159, 1166 (9th Cir. 1998). But see Mohamed v. Jeppesen Dataplan, Inc., 563 F.3d 992, 1005 (9th Cir. 2009) (state secrets privilege is a privilege "within the law of evidence" and applies only to exclude evidence—not facts; accordingly, the privilege "cannot be invoked to prevent a litigant from persuading a jury of the truth or falsity of an allegation by reference to nonprivileged evidence").

130/ United States v. Reynolds, 345 U.S. at 8.

131/ United States v. Reynolds, 345 U.S. at 11.

132/ Kasza, 133 F.3d 1159, 1166 (9th Cir. 1998).

133/ Zuckerbraun v. Gen. Dynamics Corp., 935 F.2d 544, 547 (2d Cir. 1991) ("In some cases, the effect of the invocation of the privilege may be so drastic as to require dismissal"); see also McDonald Douglas Corp. v. United States, 323 F.3d 1006 (Fed. Cir. 2003) (state secrets privilege precluded contractor's superior knowledge defense to termination for A-12 termination for default dispute).

134/ Hepting, 439 F. Supp. 2d 974.

135/ Tenet v. Doe, 544 U.S. 1 (2005).