Washington Headquarters Services

ADMINISTRATIVE INSTRUCTION

NUMBER 23
December 20, 2006

HRD

SUBJECT: Personnel Security Program and Civilian Personnel Suitability Investigation Program

References: (a) Administrative Instruction No. 23, subject as above, October 12, 1989 (hereby canceled)
(b) DoD 5200.2-R, "Personnel Security Program," January 1987
(c) DoD Directive 5110.4, "Washington Headquarters Services (WHS)," October 19, 2001
(d) Title 5, Code of Federal Regulations, Part 731, "Suitability Regulations," as amended
(e) through (y), see Enclosure 1

1. REISSUANCE AND PURPOSE

This Administrative Instruction (AI):

1.1. Reissues Reference (a) and implements guidance in Reference (b) under the authority of Reference (c).

1.2. Assigns responsibilities and prescribes procedures for administering the Personnel Security Program (PSP) and the Civilian Personnel Suitability Program (CPSP) in the Office of the Secretary of Defense (OSD) and those activities serviced by the Director, Washington Headquarters Services (WHS), under Reference (c).

2. APPLICABILITY

This AI applies to OSD, the Defense Agencies, the DoD Field Activities, and other organizational entities in the Department of Defense that receive personnel and administrative support from WHS (hereafter collectively referred to as "serviced organizations") pursuant to Reference (c).

3. POLICY

3.1. This AI implements guidance established in Reference (b). PSP, as supplemented by this AI, applies to all civilian employees, military assignees, detailees, consultants, experts, appointees, and members of commissions (hereafter referred to as "individuals").

3.2. CPSP shall be administered in accordance with Title 5, Code of Federal Regulations, Part 731 (Reference (d)).

4. RESPONSIBILITIES

4.1. The Heads of the Serviced Organizations, or their designees, shall:

4.1.1. Determine the position sensitivity for all positions within their Component in accordance with paragraph 5.

4.1.2. Ensure that all personnel within their organization are aware of the provisions of this AI.

4.2. The Director, WHS, under the authority, direction and control of the Director, Administration and Management, shall:

4.2.1. Implement Reference (b), and provide personnel security services to all serviced organizations. This includes all assigned, detailed, or employed personnel for which the Director, WHS, has been delegated responsibility or has accepted responsibility in writing for the provision of personnel security support, as authorized by Reference (c). Additionally, Reference (c) authorizes the issuing of security clearances for eligibility for access to classified information and/or occupancy of a sensitive position. It also provides the authority to deny, suspend, or revoke security clearances.

4.2.2. Implement the provisions of Reference (d) regarding a civilian employee's suitability for employment with, or retention in, the serviced organizations.

4.2.3. Be responsible for the security clearances of Congressional staff personnel, for access to classified DoD information, when requested by Congressional committee chairpersons or individual U.S. Senators and U.S. Representatives through the Assistant Secretary of Defense (Legislative Affairs) (ASD(LA)), in accordance with DoD Directive 5142.1 (Reference (e)).

4.3. The Director, Human Resources Directorate (HRD), WHS, under the Director, WHS, shall manage the PSP and CPSP through the Chief, Security Operations Division (SOD), and the Chief, Personnel Services Division. The Director, HRD, is authorized to suspend security clearances of civilian and military personnel and may delegate this authority to the Chief, SOD, pursuant to Director, Personnel and Security Directorate, Memorandum and Director, Washington Headquarters Services, Memorandum (References (f) and (g)).

4.4. The Chief, SOD, HRD, shall:

4.4.1. Initiate personnel security investigations appropriate to the designated position sensitivity after receiving a Notification of Incoming Personnel from the Personnel Services Division, the Military Personnel Division, or the Executive and Political Personnel Division within HRD.

4.4.2. Initiate investigations of Congressional staff personnel upon request of the chairperson of Congressional committees and individual senators and members of the Congress through ASD(LA).

4.4.3. Maintain security liaison with Government Agencies, including the White House, and obtain investigative information for interim clearance, reciprocal, and adjudicative purposes.

4.4.4. Grant interim security clearances in accordance with the minimum requirements of Reference (b).

4.4.5. Implement the Periodic Reinvestigation Program in compliance with Reference (b).

4.4.6. Delegate, as necessary and in the interests of program efficiency, the authority to certify security clearances for visits to other Federal Agencies and contractor facilities, process building pass requests and Joint Staff badges, conduct special access briefings, and out-process personnel to the serviced organizations' Security Managers (SMs) in accordance with Chief, Security Operations Division, Delegation of Authority (Reference (h)).

4.4.7. Maintain active and inactive OSD security files. Inactive security files shall be destroyed in compliance with AI 15 section 202-40.1 (Reference (i)) after 2 years.

4.4.8. Release security files, less investigative reports, for review by accredited investigators of other Federal Agencies.

4.4.9. Ensure reciprocal acceptance of existing security clearances or determine when additional information is required before reciprocation consideration, in accordance with Reference (b) and Executive Order 12968 (Reference (j)). Determine whether to refer a case for formal adjudication when significant information emerges subsequent to the clearance for which reciprocation is requested.

4.4.10. Maintain a case management system containing basic data on all current WHS-serviced nonsensitive and sensitive positions, including select special accesses. The Chief, SOD, shall grant access to a secure SOD operational website to duly registered SMs and select officials with appropriate need to know.

4.5. The Chief, Consolidated Adjudications Facility (CAF), HRD shall:

4.5.1. Exercise adjudication authority for the granting, denial, or revocation of personnel security clearances to all civilian personnel serviced by WHS.

4.5.2. Review, evaluate, and adjudicate background investigations, counterintelligence reports, criminal investigations, security reports, and other types of investigative information relevant to determining an individual's eligibility for a security clearance for access to classified information and/or occupancy of a sensitive position, to include Positions of Trust, in accordance with References (b) and (j). When existing reports are insufficient for adjudicative purposes, supplemental investigations or the acquisition of required information from appropriate sources may be requested.

5. PROCEDURES

5.1. Position Sensitivity and Security Clearances

5.1.1. Position Sensitivity (Civilian Personnel). The serviced organization's certifying official, as indicated in item 20, "Supervisory Certification," of Optional Form 8, "Position Description," is responsible for designating position sensitivity. The four levels of position sensitivity established by the Office of Personnel Management on Optional Form 8 and in accordance with Reference (b) shall be applied in designating the level of sensitivity for civilian personnel positions:

5.1.1.1. Nonsensitive (Position Sensitivity Designator is "1").

5.1.1.2. Noncritical-Sensitive (Position Sensitivity Designator is "2").

5.1.1.3. Critical-Sensitive (Position Sensitivity Designator is "3").

5.1.1.4. Special-Sensitive (Position Sensitivity Designator is "4").

5.1.2. Security Clearance. A security clearance represents a determination that an individual meets the standards established in References (b) and (j) for access to classified information. The type of investigation is dependent upon the designated position sensitivity. Position investigative requirements are as follows:

5.1.2.1. Nonsensitive (Position Sensitivity Designator "1"). Nominees for Nonsensitive positions, which do not require a security clearance, shall be required to submit the forms necessary for the initiation of a National Agency Check With Inquiries (NACI). NACI is the fundamental investigation for determining an individual's suitability for Federal civilian employment.

5.1.2.2. Noncritical-Sensitive (Position Sensitivity Designator "2"). Nominees for Noncritical-Sensitive positions shall be required to submit the forms for the completion of an Access NACI. Favorable adjudication shall result in the issuance of a SECRET clearance or CONFIDENTIAL eligibility.

5.1.2.3. Critical-Sensitive (Position Sensitivity Designator "3"). Nominees for Critical-Sensitive positions shall be required to submit the forms for completion of a Single Scope Background Investigation (SSBI), meeting the requirements of Reference (b) before appointment. Favorable adjudication shall result in the issuance of a TOP SECRET security clearance.

5.1.2.4. Special-Sensitive (Position Sensitivity Designator "4"). Nominees for Special-Sensitive positions are required to have an SSBI that meet the requirements of Reference (b).

5.1.3. Position Sensitivity (Military Personnel). The investigative requirements for military personnel are contained in paragraph C3.4.2. of Reference (b). The position sensitivity designators in paragraph 5.1.1. are equally applicable to military personnel. However, the adjudicative responsibility for determining a military member's eligibility for access to classified information rests with the appropriate Military Department. Military personnel selected for assignment to serviced organizations shall have the necessary investigation initiated by the losing activity prior to departure. If the military member arrives without the appropriate level of security clearance, and the losing activity has not requested the investigation, SOD shall initiate the required investigation. However, the report of investigation shall be to the appropriate Military Department for adjudication and issuance of the security clearance.

5.1.4. Exceptions to Investigative Requirements for Appointment. In an emergency, the Chief, SOD, may authorize individuals to occupy sensitive positions not initially meeting the investigative requirements for entry on duty, so long as the minimum requirements of Reference (b) are met, including an assessment that there is no available information indicating that appointment as an exception is inconsistent with the interests of national security.

5.1.5. Changes in Position Sensitivity. Position sensitivity within serviced organizations shall not be upgraded within the first 6 months of the employee's assignment to the position, for which he or she was selected or appointed initially, without a substantial change in assigned duties warranting a higher level of security clearance.

5.2. Notification of Clearance for Civilian and Military Personnel

5.2.1. Joint Clearance and Access Verification System (JCAVS). JCAVS is the DoD personnel security clearance and access database. It facilitates personnel security management for the DoD CAFs, SMs, and officers. JCAVS is maintained by the Joint Personnel Adjudication System Program Management Office. SOD serves as the senior Account Manager establishing accounts for serviced organizations. The Chief, SOD, may delegate account management to serviced organizations.

5.2.2. Security Clearance Orientation

5.2.2.1. All individuals cleared for access to classified information or assigned sensitive duties shall be given an initial security briefing by the organizational SM in accordance with Executive Order 12958, DoD 5200.1-R, and Director of Central Intelligence Directive 6/4 (References (l), (m), and (n)) as applicable.

5.2.2.2. All persons with authorized access to classified information shall sign a Standard Form (SF) 312, "Classified Information Nondisclosure Agreement," as a condition of access in accordance with DoD 5200.1-PH-1 (Reference (o)).

5.2.2.3. Individuals granted a Top Secret clearance, or component Sensitive Compartmented Information (SCI) or Special Access Program (SAP), shall attest to understanding fully their responsibilities to protect national security information and to adhering to the provisions stated on the Standard Form (SF) 312 and/or SCI/SAP Indoctrination form, after reading the entire Nondisclosure Agreement included on the form. The individual must attest orally to paragraph one of the form or agreement and it must be witnessed by one individual in addition to the official presiding over the attestation in accordance with Reference (k).

5.2.2.4. Individuals departing from serviced organizations shall report to their activity SM to complete Standard Form 416, "DoD Security Termination Statement," and any other debriefing statements relevant to non-SCI programs to which they had access.

5.2.2.5. Individuals who occupied SCI billets shall report to their activity Special Security Contact Officer (SSCO) to schedule a debriefing in accordance with Reference (b).

5.3. Periodic Reinvestigations (PRs)

5.3.1. Each civilian employee, military member, and consultant or expert, holding a security clearance for access to classified information and/or occupancy of a sensitive position shall be the subject of PR in compliance with References (b) and (j). PRs apply to civilian and military personnel.

5.3.1.1. Each individual occupying a Special Sensitive position or Critical-Sensitive position, must have a PR conducted on a 5-year recurring basis.

5.3.1.2. Individuals with SECRET security clearances must have a PR conducted on a 10-year recurring basis.

5.3.1.3. Individuals occupying Noncritical-Sensitive positions involving law enforcement and public safety duties must have a PR conducted on a 5-year recurring basis**.**

5.3.2. Upon request, all individuals under the aforementioned reinvestigation requirements are required to complete the forms necessary to initiate the appropriate PR, according to the following DoD procedures:

5.3.2.1. SOD shall send an initial electronic notification to the individual requiring the security forms necessary for the PR. A copy of this request is also sent to the individual's activity SM. The suspense shall be 30 calendar days.

5.3.2.2. If the required forms have not been submitted to SOD after 30 days, SOD shall send a second memorandum with a copy of the initial notification through the senior supervising official, to the individual, advising him or her that the requested forms have not been received.

5.3.2.3. If the forms are not received within 30 calendar days of the second written request, the Chief, SOD, shall, within 10 calendar days, notify the individual that his or her security clearance has been suspended. This memorandum shall:

5.3.2.3.1. Advise the individual as to the reason for the suspension.

5.3.2.3.2. Give the individual an opportunity to comply with the original request or furnish compelling reasons for failing to submit the required forms.

5.3.2.4. If the required security forms are not received within 30 calendar days of the date of suspension, action shall then be taken to revoke the individual's clearance as outlined in the procedures in paragraph 5.4.

5.4. Unfavorable Personnel Security Determinations

5.4.1. A final unfavorable security clearance or access determination shall not be made without ensuring the individual concerned is afforded due process rights established and in accordance with References (b) and (j). For military assignees, the authority for issuing such determinations rests with the respective Military Department (see paragraph 5.1.3.). Any unfavorable actions pertaining to military assignees will be processed through the SOD. For civilian assignees:

5.4.1.1. The individual is provided a written Statement of the Reasons (SOR) as to why the unfavorable security clearance action is being taken. The statement shall be as comprehensive and detailed as the protection of sources afforded confidentiality under the Privacy Act (Reference (p)) and national security permit; and shall provide the individual the opportunity to reply in writing to the CAF, within 30 calendar days. An extension of up to 30 calendar days may be granted by SOD, HRD, following submission of a written request from the individual. Additional extensions may only be granted by the CAF.

5.4.1.2. Failure to respond to an SOR shall result in forfeiture of all future appeal rights.

5.4.1.3. In cases resulting in a Letter of Denial or Letter of Revocation, the individual is afforded an opportunity to appeal the decision to the WHS Clearance Appeal Board either directly in writing (see paragraph 5.6) or via a personal appearance before an Administrative Judge of the Defense Office of Hearings and Appeals in accordance with paragraph C8.2.2.4.2. Reference (b).

5.4.2. The denial or revocation of a security clearance for access to classified information and eligibility to occupy a sensitive position is not a permanent bar to clearance eligibility. Therefore, based on demonstrated operational need, the agency may nominate a person whose eligibility was previously denied or revoked in accordance with WHS Security Policy, Requesting Reconsideration of Unfavorable Personnel Security Determination (Reference (q)). A period of 1 year from the date of the final decision or appeal must pass before reconsideration may occur. A request for reconsideration may be submitted to SOD through the individual's activity SM.

5.5. Suitability Determinations

5.5.1. Suitability requirements for civilian employment refer to an individual's character, reputation, trustworthiness, and fitness as related to his or her nomination for, or retention in, Federal employment as outlined in accordance with Reference (d).

5.5.2. Suitability determinations, when no adverse information is developed on nominees for employment in serviced organizations, are made in compliance with Reference (d) and upon review and adjudication of the basic forms required of all applicants, existing records of other Federal Agencies, and reports of investigations initiated by SOD and other Federal Agencies. Suitability determinations are separate and distinct from security determinations; therefore, a favorable suitability determination does not mean that the individual is eligible for a security clearance. The focus in a suitability adjudication is whether the employment or continued employment of an individual can reasonably be expected to promote the efficiency of the Federal Service. The focus of a security adjudication is the more critical question of whether the employment or continued employment of the individual reasonably can be expected to be clearly consistent with the nation's security interest. Security adjudications are made subsequent to a favorable suitability adjudication and are based on standards and criteria that include the suitability standards and criteria.

5.6. WHS Clearance Appeal Board

5.6.1. The WHS Clearance Appeal Board functions in accordance with Appendix 12 to Reference (b) and authority delegated by the Director, Administration and Management (Reference (r)). The purpose of the WHS Clearance Appeal Board is to act under the auspices of the Director, WHS, in deciding appeals of unfavorable personnel security determinations made by the WHS CAF.

5.6.2. The Board is comprised of three voting members, including a President. Additionally, the Board is supported by an Executive Secretary and Legal Counsel, who shall serve as non-voting members. Board members shall be at the civilian grade of YA-3/YC-3 or above, or the military rank of O-5 or above, and the President shall be a YC-3 or above. In the absence of the President, the Executive Secretary shall serve as Acting President.

5.6.3 Members of the Board, except the Board President, serve on an ad hoc basis and are appointed by the Board President after nomination by their employing agency or component. One member of the Board shall be a senior official of the appellant's employing agency. This ensures that the unique program and management interests of the agency are represented during Board deliberations. However, in order that the appellant receives fair and impartial consideration, this official shall not be in the appellant's supervisory chain and shall not already be familiar with case details. The third Board member shall be a senior official from OSD. Neither of these voting members may be a security professional.

5.6.4 The WHS General Counsel shall make an attorney available to provide legal counsel to Board Members during Board deliberations. In addition, the attorney shall review appeal decisions for legal sufficiency prior to issuance.

5.6.5. Appeals must be filed within the period allotted under departmental policy. Extensions of time to appeal shall be granted only when justified. The Board President shall arbitrate potential extensions. The appellant shall be notified of the decision on an extension request via his/her agency security director.

5.7. Controlled Access

5.7.1. Some individuals may, while performing their official duties, need access to sensitive information generated within or protected by offices performing certain DoD programs. These programs may involve the handling of one or more of the following types of sensitive information: North Atlantic Treaty Organization (NATO); Atomic Information (ATOMAL); Critical Nuclear Weapons Design Information (CNWDI); Single Integrated Operational Plan (SIOP); and SCI. Access to this information may be granted by heads of serviced organizations or their designees, only after the Chief, SOD, approves an appropriate request and justification; the individual reads the relevant controlled access briefing; and the individual completes the briefing certificate. Requesting officials shall include the termination date of the special access in any request. The holding of a controlled access does not automatically entitle the holder to all material bearing that controlled access designation. Organizational heads must determine need-to-know in all cases.

5.7.2. Controlled access authorizations shall be processed in the following manner:

5.7.2.1. NATO. Refers to NATO classified information at the RESTRICTED, CONFIDENTIAL, and SECRET levels in accordance with United Stated Security Authority North Atlantic Treaty Organization Instruction 1-69 (Reference (s)). "COSMIC" refers to NATO classified information at the TOP SECRET level. Access to NATO and COSMIC classified information requires a written request and justification prepared by the nominating official and forwarded in the original to the Chief, SOD. Upon a determination that the nominee meets the investigative criteria for NATO access, the nominee shall be read on by the appropriate organization SM and execute a briefing certificate. Execution of the debriefing certificate is required upon termination of the individual's need for access or departure from a serviced organization.

5.7.2.2. ATOMAL. "Restricted Data" or "Formerly Restricted Data" that is classified pursuant to the Atomic Energy Act of 1954. The requirements for the appropriate level of security clearance, requesting, briefing, and debriefing for ATOMAL special access are essentially the same as those outlined in paragraph 5.7.2.1.

5.7.2.3. CNWDI. This applies to TOP SECRET Restricted Data or SECRET Restricted Data revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition, or test device. Access to and dissemination of CNWDI is of particular concern to the Department of Defense. Because of the extreme sensitivity of this type of information, access must be limited to the absolute minimum number of individuals who need it to accomplish their assigned responsibilities. The requirements for the appropriate level of security clearance, reporting, briefing, and debriefing are found in DoD Directive 5210.2 (Reference (t). The requirements for briefing and debriefing are the same as those outlined in paragraph 5.7.2.1.

5.7.2.4. SIOP. Access to SIOP and NC2-Extremely Sensitive Information is controlled by a billet system. Access is established by organizational position and remains linked with the position until disestablished. Each billet has a unique number which identifies the position by title and lists the SIOP categories to which access is authorized for that position in accordance with Chairman of the Joint Chiefs of Staff Instruction 3231.01 (Reference (u)). The requirements for briefing and debriefing are the same as those outlined in paragraph 5.7.2.1.

5.7.2.5. SCI. Civilian, military, and contractor assignees requiring access to SCI while performing their official duties are nominated through the SOD by SSCOs within their organization. All inquiries regarding status of requests for SCI access, briefing procedures, compelling need justifications, transfer-in-status of existing access, and justifications for access shall be directed to SSCOs. The Defense Intelligence Agency (DIA) is the granting authority for access to SCI, pursuant to Reference (n). The SSCOs shall advise those individuals approved for SCI access of the procedures to follow for access briefings and debriefings within DIA.

5.8. Security Clearance Verifications

5.8.1. Within Serviced Organizations: Activities requiring verification of the security clearance held by an individual before divulgence of classified information to that individual in the course of official business may secure the verification by contacting their respective organization SM. Each SM has access to a web-based SOD clearance verification system and JCAVS.

5.8.2. Visit Requests: JPAS shall be used to verify the personnel security clearance level for visitors requiring access to classified information pursuant to Deputy Under Secretary of Defense Memorandum, "Facilitating Classified Visits within the Department of Defense" (Reference (v)).

5.8.3. Building Passes: Activity SMs are authorized to prepare and sign DD Form 2249, "DoD Building Pass Request," in accordance with Administration Instruction 30 (Reference (w)), which is the authority for all building pass procedures. When the activity determines it advantageous to OSD to issue a DoD building pass to a civilian, consultant, military, or contractor assignee meeting the requirements of Reference (w), the activity Authorized Official shall provide the individual with a completed DD Form 2249. Issuance of a DoD building pass is processed through the Pentagon Access Control Division.

5.9. Foreign Travel Briefing

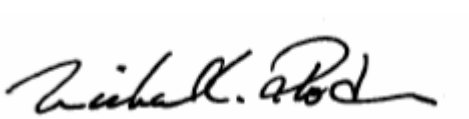
5.9.1. Cleared DoD personnel shall report any contact information or circumstances that could pose a threat to the security of U.S. personnel, DoD or other U.S. resources, classified national security information, or controlled unclassified information to the appropriate activity security manager; as directed by DoD Directive 5240.6 (Reference (x)).

5.9.2. Individuals with an SCI clearance must contact their activity SSCO for required counterintelligence briefs before overseas travel (Reference (n)).

5.9.3. All DoD personnel contemplating travel overseas shall attend a travel briefing at least annually, from a certified Anti-Terrorism/Force Protection instructor. Individuals requiring a briefing should contact their serviced organizations' SM and/or the Pentagon Force Protection Agency in accordance with DoDI 2000.16 (Reference (y)).

6. EFFECTIVE DATE

This AI is effective immediately.



Michael L. Rhodes
Director

Enclosures- 1
E1. References, continued

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD Directive 5142.01, "Assistant Secretary of Defense for Legislative Affairs (ASD(LA))," September 15, 2006
(f) Director, Personnel and Security Directorate Memorandum, Delegation of Authority, April 19, 2000[1]
(g) Director, Washington Headquarters Services Memorandum, Delegation of Authority, December 3, 1993
(h) Chief, Security Operations Division, "Delegation of Authority," December 21, 1998
(i) Administrative Instruction 15, "Office of the Secretary of Defense Records Management Records Disposition Schedules," Volume II, August 11, 1994
(j) Executive Order 12968, "Access to Classified Information," August 4, 1995
(k) Director, Administration and Management Memorandum, "Delegation of Authority," April 28, 1995
(l) Executive Order 12958, "Classified National Security Information," April 17, 1995
(m) DoD 5200.1-R, "Information Security Program," January 14, 1997
(n) Director of Central Intelligence Directive 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)," October 13, 1999
(o) DoD 5200.1-PH-1, "Classified Information Nondisclosure Agreement (SF-312)," May 2000
(p) Section 552a of title 5, United States Code
(q) WHS Security Policy Memorandum, "Requesting Reconsideration of Unfavorable Personnel Security Determination," March 28, 1997
(r) Director, Administration and Management Memorandum, "Component Appeals Board," January 11, 1995
(s) United Stated Security Authority North Atlantic Treaty Organization, Instruction 1-69, "United States Implementation of NATO Security Procedures (U)," April 21,1982
(t) DoD Directive 5210.2, "Access to and Dissemination of Restricted Data," January 12, 1978
(u) Chairman of the Joint Chiefs of Staff Instruction 3231.01, "Safeguarding the Single Integrated Operational Plan (SIOP)," January 7, 2000
(v) Deputy Under Secretary of Defense for Intelligence Memorandum, "Facilitating Classified Visits within the Department of Defense," April 1, 2005
(w) Administrative Instruction O-30, "Security for the Pentagon Reservation," June 5, 2002
(x) DoD Instruction 5240.6, "Counterintelligence (CI) Awareness, Briefing, and Reporting Programs," August 7, 2004
(y) DoD Instruction 2000.16, "DoD Antiterrorism (AT) Standards," October 2, 2006

[1]References (f), (g), (h), (k), and (q) are available in the WHS, HRD, Security Operations Division