Recent Developments

Security Clearance Changes and Confusion in the Intelligence Reform Act of 2004

Sheldon I. Cohen*

The Intelligence Reform and Terrorism Prevention Act of 2004[1] (the "Act") effected one of the most significant changes since 1947 in the organization of the intelligence community. Title III of the Act reorganized the entire national security clearance system,[2] although the subject received practically no attention in public discussion during the 9/11 Commission hearings. Because this change was not fully explored in either the House or Senate hearings or during floor debate, Title III includes contradictory provisions concerning the assignment of responsibilities for security clearance policies and procedures.

The origin of the security clearance reorganization is found in a recommendation of the 9/11 Commission aimed at accelerating the processing of appointments to national security positions. The Commission was concerned that a catastrophic attack on the United States during the transition from one administration to another could severely disrupt national security preparedness.[3] It recommended that

> [a] single federal agency should be responsible for providing and maintaining security clearances, ensuring uniform standards – including uniform security questionnaires and financial report

---

* The author is in private practice in Arlington, Virginia. He is the author of *Security Clearances and the Protection of National Security Information: Law and Procedures*, published by the Defense Personnel Security Research Center, Technical Report 00-4 (2000). It is available online from the United States National Technical Information Center, www.ntis.gov, Accession Number ADA 388100. The author may be contacted at www.sheldoncohen.com

1. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638.

2. Title III of the Act, entitled "Security Clearances," is codified at 50 U.S.C.A. §435b (West Supp. 2005). References hereinafter are to sections of the Act as codified.

3. NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 422 (2004).

> requirements, and maintaining a single database. This agency can also be responsible for administering polygraph tests on behalf of organizations that require them.[4]

This recommendation resulted in House and Senate bills containing somewhat similar provisions to reform our national intelligence structure.[5] The Act, as passed, calls for reciprocity of security clearance and access determinations, establishment of a national database, use of all available technology in clearance investigations, and reduction in the length of time required for personnel security clearances to be investigated and adjudicated.

Under the new law, the President must select a single office (the "Entity") that will be responsible for overall security clearance direction and policy.[6] Title III of the Act requires the President, within ninety days after its enactment, to designate a department, agency, or other element of the executive branch, to: (1) direct day-to-day oversight of investigations and adjudications for personnel security clearances; (2) develop and implement uniform and consistent policies and procedures for completion of security clearances and access determinations for highly sensitive programs; (3) serve as the "final authority" to designate an authorized investigative agency or authorized adjudicative agency; (4) ensure reciprocal recognition of access to classified information among agencies of the federal government; (5) ensure, "to the maximum extent practicable," that sufficient resources are available in each agency to achieve clearance and investigative program goals; and (6) review and coordinate the development of tools and techniques for enhancing the conduct of investigations and the granting of clearances.[7]

The Act further directs the President, in consultation with the head of the Entity, not later than 180 days after enactment, to select a single agency in the executive branch to conduct, "to the maximum extent practicable," security

---

4. *Id.* Recommendations designed to promote "greater uniformity, reciprocity, and cost effectiveness in the clearance process" had been offered earlier by the Moynihan Commission. *See* REPORT OF THE COMMISSION ON PROTECTING AND REDUCING GOVERNMENT SECRECY 82 (1997).

5. *Compare* H.R. 10, 108th Cong. §§5071-5078 (2004), *with* S. 2845, 108th Cong. §116 (2004).

6. 50 U.S.C.A. §435b(b). The House Bill would have created a new position, Deputy National Intelligence Director for Community Management and Resources, to be responsible for oversight of the security clearance process. H.R. 10, *supra* note 5, §5072. It also would have required the President-elect to submit the names of candidates for high level national security positions as soon as possible after the date of the general election for President and before the inauguration. *Id.* §5077.

7. 50 U.S.C.A. §435b(b).

clearance investigations for both federal employees and contractor personnel.[8] However, the head of the Entity may also designate other agencies to conduct investigations if it is considered "appropriate for national security and efficiency purposes."[9] Thus, the agency selected to conduct investigations will have sole authority, except when the head of the Entity directs otherwise. What the Act giveth, the Act taketh away.

Currently there are numerous investigative agencies, including the Defense Security Service (DSS), the Office of Personnel Management (OPM), the FBI for its personnel, as well as each of the intelligence agencies. There are also multiple adjudicative agencies, including the Defense Office of Hearings and Appeals (DOHA) for government contractors, and eleven DOD Central Adjudicative Facilities for military personnel and civilian employees. Each intelligence agency also has its own adjudication facility.[10] Since the Act allows the head of the Entity to designate other agencies to conduct investigations on highly flexible terms, there is a substantial risk that the current fragmented clearance process will continue.

There are further incongruities in the Act. As indicated above, the statute directs the President to select a single entity to be responsible for developing and implementing uniform and consistent policies and procedures for security clearances and determinations for access.[11] However, the Act also gives the newly-created Director of National Intelligence the authority to "establish uniform security standards and procedures."[12] Since the head of the Entity

---

8. *Id.* §435b(c)(1).

9. *Id.*

10. Some feel that the Act does not affect DOHA or its adjudication of government contractors' security clearances. They point to 50 U.S.C.A. §435b(a)(3), which defines the term "authorized adjudicative agency" as an agency authorized to "determine eligibility for access to classified information in accordance with Executive Order 12968." Section 7(c) of Executive Order 12,968, *Access to Classified Information,* 60 Fed. Reg. 40,245 (Aug. 7, 1995), provides that that order does "not diminish or otherwise affect the requirements of Executive Order 10,450." Exec. Order 10,450, *Security Requirements for Government Employment*, 18 Fed. Reg. 2,491 (Apr. 29, 1953), prescribes procedural rights for government contractors that are not available to government employees, applicants, or military personnel, due to an historical quirk. *Compare* Greene v. McElroy, 360 U.S. 474, 496 (1959), *with* Vitarelli v. Seaton, 359 U.S. 535 (1959), *and* Dept. of Navy v. Egan, 484 U.S. 518 (1988). Since the earlier executive order provides that DOHA shall adjudicate contractor hearings, some argue that DOHA is exempt from the Act. However, Executive Order 12,968 establishes broad adjudicative standards and principles that apply to DOHA and government contractors as well as to all others needing security clearances.

11. 50 U.S.C.A. §435b(b).

12. *Id.* §403-1(g)(1)(A); *see also id.* §403-1(j) (directing the DNI to establish uniform procedures for the granting of access to sensitive compartmented information).

does not report to the Director of National Intelligence, how these responsibilities will be divided is anyone's guess.[13]

The Entity is responsible for day-to-day oversight of investigations and adjudications of all personnel security clearances, including "highly sensitive programs."[14] Such programs include Special Access Programs (SAPs)[15] and Restricted Data programs under the Atomic Energy Act administered by the Department of Energy. They also include Sensitive Compartmented Information (SCI), access to which is now controlled under guidelines issued by the Director of Central Intelligence.[16]

Until now, the agencies controlling these highly sensitive programs have been adamantly opposed to relinquishing control of their personnel security clearances, and they have declined to recognize each other's clearances, resulting in new investigations, new polygraph tests, and new standards each time a person moves from one program to another. This reluctance has sometimes resulted in a clearance being granted by one agency and denied by another with no change in the circumstances of the person under consideration – all despite the establishment of uniform guidelines for determining eligibility for access to classified information[17] under a 1995 executive order that remains in force.[18]

The Act now requires that all security clearance background investigations and determinations completed by an authorized investigative agency or

---

13. The author is not a alone in his confusion. Porter Goss, Director of the CIA, has said of the Act: "It's got a huge amount of ambiguity in it. I don't know by law what my direct relationship is with John Negroponte." NBC NEWS TRANSCRIPTS, March 3, 2005. Negroponte is the first DNI.

14. 50 U.S.C.A. §435b(b)(1).

15. A Special Access Program is "a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level." Exec. Order 12,958, *Classified National Security Information*, §4.1(h), 60 Fed. Reg. 19,825, 19,836 (Apr. 20, 1995).

16. Director of Central Intelligence Directive 6/4, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)*, Oct. 13, 1999 [hereinafter DCID 6/4], at Annex C, *available at* http://www.fas.org/irp/offdocs/cid6-4/.

17. *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*, 32 C.F.R. pt. 147 (2005). The guidelines are incorporated verbatim into DCID 6/4, Annex C, *supra* note 16.

18. Exec. Order No. 12,968, *supra* note 10. Among many examples in the author's experience, the National Security Agency, a DOD component, refused to accept the Top Secret clearance of a Navy employee detailed to NSA, and the CIA refused to accept an employee from the Department of Defense holding a Top Secret clearance, although there was no new or derogatory information on either employee.

authorized adjudicative agency be accepted by all other agencies.[19] Yet despite its call for "ensuring reciprocal recognition,"[20] the Act does not require that there be a single clearance determination binding on all agencies. If there is a dispute between agencies arising from an agency's refusal to recognize another agency's clearance or access determination, the Entity will act as the final authority to arbitrate and resolve the dispute.

It remains to be seen how well this will work. Any arbitration will take place between agencies, and the individual concerned probably will have no standing to initiate an arbitration. An agency will need a great interest in one of its employees or contractor employees having access to another agency's information to demand arbitration. Faced with an interagency arbitration, the sponsoring agency could just as easily send another person to fill the slot. Moreover, while the Act provides that an authorized investigative agency's background investigations are transferable to any other authorized investigative agency,[21] it is hard to imagine an intelligence agency or DOE willingly giving up to OPM, to DSS, or even to another intelligence agency, its authority to conduct its own investigations.

Uniform standards and procedural requirements are currently specified in Executive Order No. 12,968[22] and uniform guidelines for determining eligibility for access have been issued under that order.[23] These requirements and the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information have most recently been revised at the direction of the President, for immediate implementation.[24] The Act directs that an authorized

---

19. 50 U.S.C.A. §435b(d)(1).

20. *Id.* §435b(b)(4).

21. *Id.* §435b(d)(2). In February 2005, the Defense Security Service transferred its investigative functions and investigating resources to the Office of Personnel Management. *See* DSS Industrial Security Letter No. 05L-1, Jan. 18, 2005, at 3, *available at* http://www.dss.il/isec/ISL05L-1.pdf. OPM thus inherited 1,578 investigators, managers, and support staff, and a backlog of 146,288 cases in the process for completion. Of those, 101,351 cases were past due and more than 35,000 had been in process for more than 120 days. OPM hopes to reduce the time for completion of the investigation from three years to 60-90 days. OPM Responses to Inquiry (on file with author).

22. *Supra* note 10.

23. *See supra* note 17.

24. Memorandum for William Leonard, Director, Information Security Oversight Office, from Steven J. Hadley, Assistant to the President for National Security Affairs, *Adjudicative Guidelines*, Dec. 29, 2005, *transmitting Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*, *available at* http//www.fas.org/sgp/isoo/guidelines.html; *see also* Memorandum for Deputies of Executive Departments and Agencies from Clay Johnson III, Deputy Director for Management, Office of Management and budget, *Reciprocal Recognition of Existing Personnel Security Clearances*, Dec. 12, 2005, *available at* http://www.fas.org/sgp/thergov/reciprocal.pdf.

investigative agency or an authorized adjudicative agency may not establish additional requirements which exceed the current executive order (other than for the conduct of a polygraph), except as the head of the Entity considers necessary for national security purposes.[25]

The goal of reciprocal recognition of clearances and access is advanced in other ways. The Act requires that a background investigation and clearance determination completed by an "authorized investigative agency or authorized adjudicative agency" be accepted by all other agencies.[26] Background investigations started by one authorized investigative agency are transferrable to another.[27] An authorized investigative or adjudicative agency also may not conduct an investigation or an adjudication to determine whether to grant a security clearance to an individual if a current investigation or clearance of an equal level already exists or has been granted by another authorized adjudicative agency.[28] Yet the head of the Entity may decide that a new investigation and determination is "necessary for national security purposes."[29] In fact, the Act directs the head of the Entity to establish a procedure to allow an agency to challenge a reciprocity requirement.[30]

A centralized database is to be established within twelve months after enactment of the Act.[31] It is to be operated by the Office of Personnel Management. The database will record the granting, denial, and revocation of security clearances for all military, civilian, or government contractor personnel from all authorized investigative and adjudicative agencies. It is to integrate existing federal clearance tracking systems, such as the Defense Clearance and Investigations Index (DCII) maintained by DOD and the Security Investigations Index (SII) maintained by OPM. The establishment of this database was underway even before the Act was adopted, but it not clear to what extent independent databases, such as those maintained by the intelligence agencies or the FBI, have thus far been integrated into the new one.

The serious problem of delay in investigating and adjudicating clearances is finally addressed in the Act. A 2004 GAO report estimated that DOD's

25. 50 U.S.C.A. §435b(d)(3).
26. *Id.* §435b(d).
27. *Id.* §435b(d)(2).
28. *Id.* §435b(d)(4).
29. *Id.* §435b(d)(5).
30. *Id.* §435b(d)(6).
31. *Id.* §435b(e).

backlog of overdue investigations was approximately 360,000 cases.[32] Investigations have been transferred from DSS to OPM and back again in an effort to reduce the backlog. Cases languish for two or more years during the course of a routine investigation, and if they are referred for adjudication they may be delayed for more than a year at DOHA before appeals are exhausted, or twice that long at the CIA. In the meantime, government and contractor personnel cannot be assigned to the tasks for which they were hired, persons whose clearances have been suspended are put on indefinite unpaid leave until there is a final adjudication, employees move on to other jobs because they get tired of waiting, and contractor employees just get fired.

The Act tries to address this problem by requiring the head of the Entity to develop a plan that will require the completion of determinations for 90 percent of all applications within an average 60 days following receipt of each completed application.[33] Not more than 40 days is to be used for an investigation and not more than 20 days for an adjudication. This sounds like a bold move forward until one does the numbers. Ten percent of the applications are not included in the average and have no time limit, except that they "shall be made without delay."[34] Of the 90 percent required to be completed within the 60 day "average," a substantial number, perhaps half or more, will take more than 60 days. The natural effect on any agency trying to meet its numbers requirement will be to put the easy ones in the front of the queue, leaving the more difficult ones to fall farther and farther behind. Moreover, the plan to speed up the process will not take effect until December 2009.[35]

CONCLUSION

What has the Act accomplished? For one thing, there now will be someone in charge of the entire security clearance process. The last time the National Industrial Security Program was revised was in 1993. The last time the relevant executive order and personnel security guidelines were revised,

---

32. U.S. GEN. ACCOUNTING OFFICE, DOD PERSONNEL CLEARANCES: DOD NEEDS TO OVERCOME IMPEDIMENTS TO ELIMINATING BACKLOG AND DETERMINING ITS SIZE 8, 26 (2004), *available at* http://www.gao.gov/new.items/d04344.pdf.

33. 50 U.S.C.A. §435b(g)(1), (2). The House Bill would have required a determination on all applications within 60 days. H.R. 10, *supra* note 5, §5076.

34. 50 U.S.C.A. §435b(g)(2)(B).

35. *Id.* §435b(g)(3)(A). There will be some implementation before that time. Within two years after enactment, by December 2006, each adjudicative agency must complete 80 percent of its adjudications within 120 days after receipt of the completed application, including 90 days to complete the investigation and 30 days to complete the adjudication. *Id.* §435b(g)(3)(B).

it was done by an interagency drafting committee in 1995. Until now the Director of the CIA, wearing the hat of Director of Central Intelligence, set the standards for SCI access.[36] DOD set the standard for virtually every other agency, except the FBI and DOE, which went their own ways.[37] The single Entity is now expected to coordinate and direct the entire process.

What is not likely to be accomplished? For every new requirement imposed by the Act, there seems to be an out. The Entity is to ensure that sufficient resources are available to meet program goals, but only "to the maximum extent practicable."[38] The President is to select a single agency in the executive branch to conduct security clearance investigations, but again only "to the maximum extent practicable."[39] The head of the Entity may designate other agencies to conduct investigations if he or she "considers it appropriate for national security and efficiency purposes."[40] The Act calls for "ensuring reciprocal recognition of access to classified information" among agencies, but it allows for arbitration to resolve disagreements.[41] All of the Act's requirements for reciprocity may be overridden when the entity head determines it to be necessary for national security purposes.[42] And the prescribed plan to accelerate the security process, to be implemented in 2009, need only require determination of 90 percent of clearance applications within an average of 60 days "[t]o the extent practical," leaving others to be made "without delay."[43]

Nevertheless, all of the elements of the new organizational structure called for in the Act currently exist, and it is hard to imagine that these elements will not be utilized in some form to meet the statutory requirements. The primary

---

36. DCID 6/4, *supra* note 16, is the government standard for SCI.

37. DOD Dir. 5200.2, *DoD Personnel Security Program*, Apr. 9, 1999, *available at* http://rimr. atrc.org/PolicyLibrary/DoD/5200.2(1).pdf, and DOD Reg. 5200.2-R, *Personnel Security Program*, Jan. 1, 1987, *available at* http://www.dtic.mil/whs/directives/corres/html/52002r.htm, establish the personnel security program for DOD and its agencies. These standards are applied by DOHA to its contractor adjudications and to contractors of twenty other agencies under DOD Dir. 5220.6, *Defense Industrial Personnel Security Clearance Review Program*, Jan. 2, 1992, *as amended*, *available at* http://www.dtic.mil/whs/directives/corres/ html/52206.htm, and an agreement with the other agencies. *See id.* §2.2 (listing the agencies). The Nuclear Regulatory Commission's regulations are at 10 C.F.R. pt. 10 (2005). The FBI's background investigations of its employees are conducted in accordance with Part 67 of the FBI Manual of Investigative Operations and Guidelines (MIOG). The MIOG is not publically available, but was provided to the author in response to a request under the Freedom of Information Act.

38. 50 U.S.C.A. §435b(b)(5).

39. *Id.* §435b(c)(1).

40. *Id.*

41. *Id.* §435b(b)(4).

42. *Id.* §§435b(d)(3)(B), 435b(d)(5).

43. *Id.* §435b(g)(2).

organization for resolving contractor clearances is DOHA, and it will most likely continue to have that responsibility. The various central adjudication facilities, with their experienced personnel and institutional knowledge, will certainly be retained, and they may be consolidated in some fashion to serve as a single adjudicative body for collateral clearances for military personnel and civilian government employees. There could be a consolidation of access determinations for the "highly sensitive programs," such as SCI, Restricted Data under the Atomic Energy Act, and Special Access Programs. Indeed, all organizations and personnel currently involved with security investigations and access determinations will probably be included in whatever new structure results from the Act.

Government personnel in some "sensitive" positions who do not deal with classified national security information, but who instead are exposed to essential parts of the government infrastructure, such as electronic databases and networks, and to information concerning the nation's industrial base, may also be affected by the Act. While the Act does not address "suitability" determinations (background reviews) for these individuals, such determinations could be included in the centralized structure for security determinations.

With all the loopholes in the Act and opportunities for delay and obstruction, the goals of standardization and reciprocity can only be achieved if there is cooperation among the affected agencies. Unfortunately, history does not give us much reason to hope for such cooperation. A strong Entity will be needed to avoid turf battles and resolve disputes. If standardization and reciprocity are not achieved, the goal of the 9/11 Commission – to streamline the security clearance process and get critical personnel in place quickly – will not be met.

* * *