
BY THE U.S. GENERAL ACCOUNTING OFFICE

Report To The Secretary Of Defense

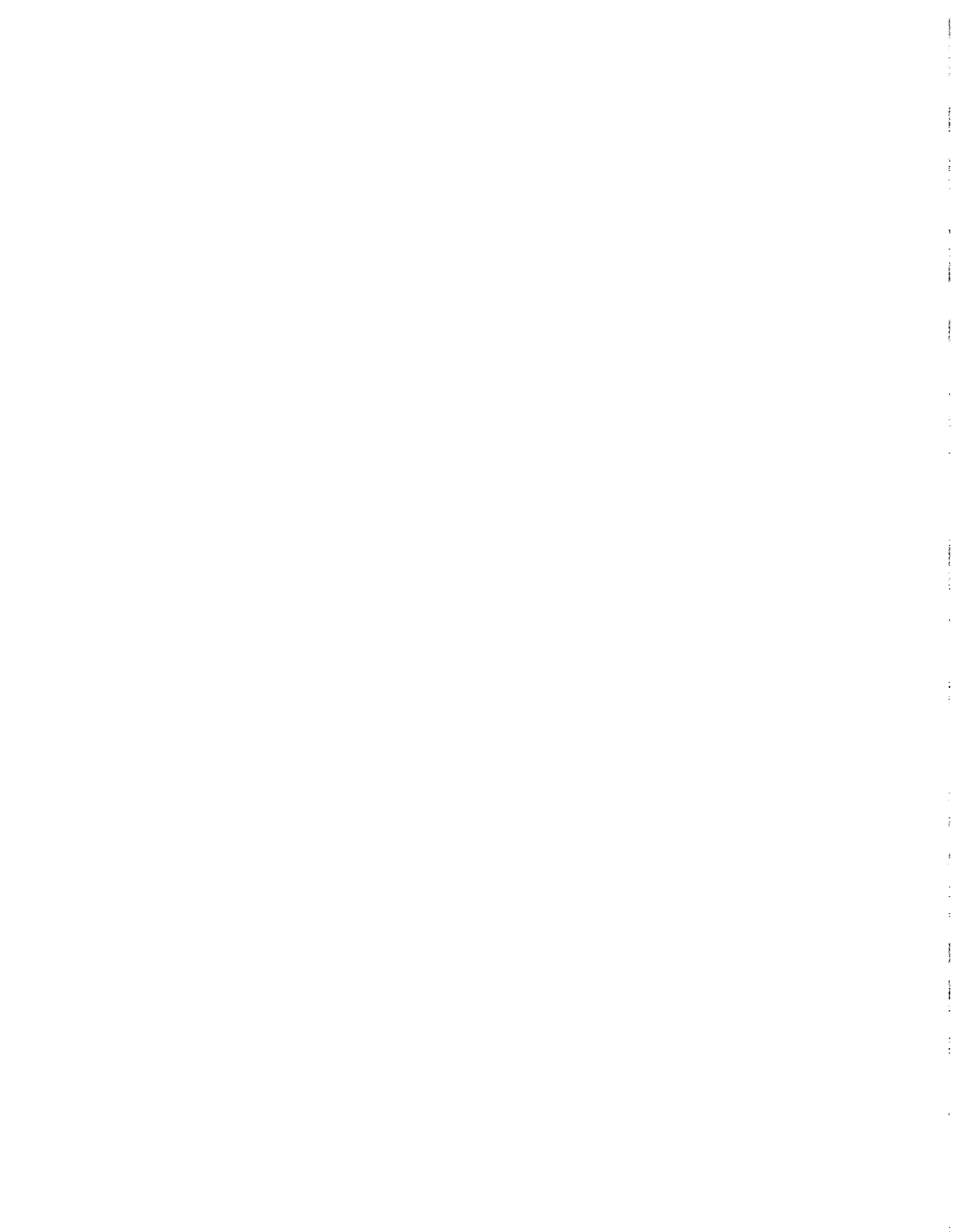
Further Improvements Needed In Department Of Defense Oversight Of Special Access (Carve-Out) Contracts

Special access contracts, including carve-out contracts for which the Defense Investigative Service does not make security inspections, require special and costly measures to protect especially sensitive information. GAO found that some contracts were given carve-out status for reasons other than security, and other carve-out contracts were not inspected by anyone.

This report recommends actions that the Department should take to improve oversight of special access contracts. The Department's comments and GAO's evaluation are included in a separate report supplement (GAO/GGD-83-43 (A)) because the Department marked the comments "FOR OFFICIAL USE ONLY" and requested that GAO exempt the information from public disclosure. It is GAO's policy to observe such requests.



GAO/GGD-83-43
FEBRUARY 18, 1983





UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

GENERAL GOVERNMENT
DIVISION

B-210341

The Honorable Caspar W. Weinberger
The Secretary of Defense

Attention: Director, GAO Affairs

Dear Mr. Secretary:

The General Accounting Office has completed a review of security requirements and administration of Department of Defense (DOD) carve-out contracts, as part of our continuing review of national security information, requested by the Chairman, Subcommittee on Government Information and Individual Rights, House Committee on Government Operations. Carve-out contracts are those special access contracts for which the Defense Investigative Service (DIS) has been relieved of security inspection responsibility under the Defense Industrial Security Program. In such cases, the cognizant DOD component is responsible for security inspections and administration.

The objective of the Defense Industrial Security Program is to protect classified information held by industry and is applicable to all DOD components and other Government agencies that enter into agreements with DOD. The program is administered by DIS on behalf of all DOD and other agency users. Prior to August 1965, program implementation, or security cognizance as it is referred to, was the responsibility of each military department. Since establishment of centralized security cognizance, the number of carve-out contracts has continually increased.

The ever-increasing number of carve-out contracts has become a problem for contractor security administrators because the contracts result in a multiplicity of security requirements in addition to those prescribed by DOD's Industrial Security Manual. The exact number of carve-out contracts is unknown but, on the basis of available data, we estimate that there probably are several thousand such contracts.

We directed our review primarily to Army, Navy, and Air Force carve-out contracts because of the large number of such contracts issued by the military services. We visited 40 contractors and 20 DOD offices and installations in Alabama,

California, Florida, Maryland, and Virginia. We selected contractors on the basis of their size and activity with the services. We reviewed regulations and instructions, contract security specifications, inspection reports, and other administrative documentation and interviewed DOD and contractor personnel. This review was made in accordance with generally accepted Government auditing standards.

Briefly, we found that DOD needs to (1) establish oversight procedures for carve-out contracts entered into by the military services; (2) improve implementation of uniform construction standards for sensitive compartmented information facilities; (3) centralize and improve security inspections of sensitive compartmented information facilities and special access contracts; and (4) improve the process for advance DOD approval of contractors' requests for employee special access authorizations that require special background investigations. These findings are discussed in detail in the appendix.

On pages 6, 8, 11, and 13 of the appendix we are recommending that you

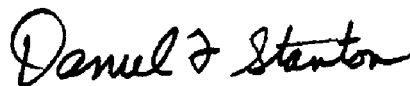
- revise the Information Security Program Regulation to require all components to annually (1) inventory and report the status of all carve-out contracts to the Deputy Under Secretary of Defense for Policy and (2) revalidate the need for renewed contracts or contracts that extend for more than 1 year;
- require the Office of the Deputy Under Secretary of Defense for Policy to make periodic inspections of components' central offices to evaluate compliance with the regulation;
- direct the Defense Intelligence Agency (DIA) to revise its regulations to require that a threat analysis be made before a sensitive compartmented information facility (SCIF) is constructed or altered or an existing facility is approved for use as a SCIF;
- make DIA responsible for approving all industry facilities proposed for use as DOD SCIFs;
- make DIS responsible for (1) inspecting all DOD sponsored contractor SCIFs and (2) verifying accountability for all contract documents maintained in those SCIFs and in SCIFs sponsored by other agencies;

- issue instructions that will require advance DOD approval of contractors' requests for special access authorizations for employees who will be working on non-SCI special access contracts;
- direct DIS to return to contractors any requests for special access authorizations that do not contain the advance approval of the cognizant DOD component; and
- remind DOD components of their responsibility to review and approve, in a timely manner, contractor nominees for all special access authorizations.

By letter dated January 21, 1983, the Deputy Under Secretary of Defense for Policy commented favorably on most of our findings and recommendations. The comments and our evaluation are not enclosed with this report because the comments are marked "FOR OFFICIAL USE ONLY" (FOUO) and DOD has requested that "GAO impose safeguards to prevent unauthorized access and to exempt the information from public disclosure." It is our policy to observe an agency's administrative markings and safeguard the information according to the originating agency's requirements. However, a supplement to this report, with the comments and our evaluation, will be provided to requestors in accordance with the provisions of DOD Directive number 5400.7: DOD Freedom of Information Act Program, dated March 24, 1980. That directive provides for dissemination of material marked FOUO within Government and industry to conduct official business.

We are sending copies of this report to the Chairman, Subcommittee on Government Information and Individual Rights, House Committee on Government Operations; Director, Office of Management and Budget; and the Director, Information Security Oversight Office. As you know, 31 U.S.C. §720 requires the head of a Federal agency to submit a written statement on actions taken on our recommendations to the Senate Committee on Governmental Affairs and the House Committee on Government Operations not later than 60 days after the date of the report and to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of the report.

Sincerely yours,



For William J. Anderson
Director

GAO REVIEW OF DOD SPECIAL ACCESS CONTRACTS
BACKGROUND, FINDINGS, AND RECOMMENDATIONS

BACKGROUND

According to Executive Order 12356 and its implementing directive, which took effect August 1, 1982, special access programs may be created by agency heads when (1) normal management and safeguarding procedures do not limit access sufficiently and (2) the number of persons with access is limited to the minimum necessary to meet the objective of providing extra protection for the information. With respect to DOD, agency heads include the Secretaries of Defense, Army, Navy, and Air Force. The new order's requirements are similar to those of the previous order that was in effect from December 1, 1978, through July 31, 1982. Both orders provide that special access programs pertaining to intelligence activities need the approval of the Director of Central Intelligence.

Most special access programs involve industry support which means that special handling of sensitive, classified information and limited contractor employee access are required. The majority of these special access contracts are carve-out contracts; consequently, DIS does not make periodic security inspections. Some special access contracts that do not support special access programs have also been carved out. There are two basic types of carve-out contracts: those that involve intelligence or intelligence-related information and those that do not.

Intelligence or intelligence-related information that requires special handling is referred to as sensitive compartmented information (SCI). A special facility known as a sensitive compartmented information facility (SCIF) is required for the storage of SCI. Every contractor-operated DOD SCIF has a DOD component as a sponsor. Many SCIFs are also used by other components who are tenants. Many contractors have more than one SCIF. One contractor that we visited had 10 SCIFs. The cost to construct a SCIF ranges from \$10,000 to \$1,000,000, depending upon its size and location within an existing building or in a building to be constructed and requirements of the sponsor. Some SCIFs may be only a small room. Others may occupy as much as 40,000 square feet. If the SCIF is to contain automatic data processing equipment or word processors, the cost of the facility can run as high as \$126 a square foot because of the extra protection that is required.

The Defense Intelligence Agency (DIA) has issued standards for the construction of DOD SCIFs, including those in

industry, based on standards prescribed by the National Foreign Intelligence Board. DIA has also issued a security administration manual for contractors who handle SCI. In July 1982, DOD had about 1,400 SCI contracts with several hundred contractors. About 12,000 contractor employees were cleared to work on those contracts, according to figures supplied by DOD components.

There are no uniform DOD standards for the storage and handling of nonintelligence-related special access program information. However, because of its sensitivity, some nonintelligence-related information is maintained in SCIFs or in other special facilities required by DOD components. All SCI contracts are carved out. Some special access contracts with nonintelligence-related information are not carved out; DIS is responsible for security administration of those contracts. However, security administration for most non-SCI special access contracts has been retained by the DOD components that awarded the contracts. The number of non-SCI carve-out contracts was unknown because two major DOD components had not established centralized control over the issuance of carve-out contracts. One major component, for security reasons, was reluctant to provide us the information.

FINDINGS

OVERSIGHT PROCEDURES NEEDED FOR CARVE-OUT CONTRACTS

DOD revised its Information Security Program Regulation, effective August 1, 1982. This regulation contains policy and procedures for the establishment of special access programs and their supporting carve-out contracts; however, the regulation does not give DOD the necessary oversight of new carve-out contracts or of existing contracts that may be renewed by the military services. Consequently, even though the revised regulation is an improvement, there is no assurance that past abuses in the establishment of some carve-out contracts will be eliminated or, even more important, that the large number of carve-out contracts can be reduced or eliminated to allow DIS to perform the centralized inspection function that was intended when the Defense Industrial Security Program was revised in 1965.

During one 12-month period, the headquarters office of one military service, responsible for recommending approval of SCI carve-out contracts on the basis of established criteria, recommended that 22 contracts not be granted carve-out status. When these recommendations were reviewed by higher authority within the service, the recommendations were overruled and the 22 contracts were carved out.

Contrary to the regulations of one service, three non-SCI carve-out contracts were established without the headquarters office's approval. They were identified during our review and the headquarters office later approved the carve-out status of the contracts.

Level of security inconsistent with justification for carve-out contracts

We found indications that security may not have been the primary reason for some contracts being carved out. There was inconsistency in the establishment of many of the non-SCI carve-out contracts because of the level of classification of the contracts and the security clearance level of contractor employees with access to contract information.

Many non-SCI carve-out contracts were classified at the secret level. Classification of the contracts at that level raises a question as to the justification for the contracts being carved-out. It seems to us that if the information involved with the contracts was so sensitive that it had to be excluded from the Defense Industrial Security Program, then, perhaps, it should have been classified at the top secret level. According to Executive Order 12356 and its predecessor, the secret classification is to "be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security." Similarly, the top secret classification is to be used when "exceptionally grave damage" is likely to result from the unauthorized disclosure of the information.

Complete statistics on the number of contractor employees authorized to work on non-SCI special access contracts were unavailable because not all non-SCI contracts were controlled on a centralized basis by the military services. However, the headquarters offices of the military services told us that about 39,000 contractor employees, including 20,000 associated with one program, had been given special access authorizations to non-SCI contracts. Of the 39,000 employees, about 13,500 had security clearances at the secret level. One DOD official estimated that over 150,000 contractor employees had been authorized by DOD components to work on special access contracts, including about 12,000 employees involved with SCI contracts.

The special access authorizations given to the employees are in addition to their top secret and secret security clearances. A secret level security clearance generally is issued on the basis of a favorable national agency check (NAC). The NAC involves a review of Federal Bureau of Investigation and other investigative agency records to determine the existence of any records of arrest.

A top secret clearance generally is issued on the basis of a favorable background investigation. That investigation consists of a NAC; records checks at local law enforcement agencies, places of employment, and educational institutions; and interviews with individuals who are or have been acquainted with the employee being investigated. The investigation generally covers the previous 5-year period or as far back as the employee's 18th birthday, whichever comes first.

Generally, all employees with access to SCI and some employees with access to non-SCI information are permitted such access only on the basis of a favorable special background investigation. The special background investigation is similar to the background investigation required for a top secret clearance except that the period of time covered by the special investigation is 15 years.

We were told that many employees with only secret clearances and access to non-SCI carve-out contracts did administrative and maintenance work and did not have access to classified contract information. Nevertheless, one contractor had about 500 employees with secret clearances, who had access to non-SCI carve-out information. Another contractor, with non-SCI carve-out contracts, told us that about 100 employees with secret clearances had access to contract information.

We believe that it is inconsistent to exclude, for security reasons, DIS inspections by inspectors with top secret clearances based on background investigations, while permitting access by contractor employees with only secret clearances based on national agency checks.

Security justification of other carve-out contracts also questionable

The following examples also illustrate the questionable establishment of some carve-out contracts justified on the basis of security.

One contractor told us that the reason for one service's carve-out contract was to keep another service from knowing about the project and its sponsor rather than to ensure the security of the information. We did not discuss this point with the sponsoring service because contractors were promised anonymity in their discussions with us.

Another contractor told us that the purpose of one contract was to evaluate the work done by other contractors. Although we did not review the justification for the contract being carved out, it appeared to us, and the contractor concurred, that adequate security probably could be provided by

strictly limiting access to the contract and related documents. It also appeared to us that DIS could have been making security inspections of the special facility and contract.

Two contractors told us that for their contracts, only the contract documents themselves were carved out. The statements of work and documents related to contract performance were not carved out. One of the contractors thought that the reason for this unusual arrangement was to preclude someone from identifying the military service involved and the amount of money being spent.

Another contractor said that a contract was carved out to expedite procurement. The contractor told us that, initially, precontract award lead time was estimated to be 2 years. After the contract was carved-out, the lead time was reduced to 6 months. Several contractor and DOD officials told us that they thought that carve-out contracts were being used to expedite procurements and facilitate sole source awards.

Revisions to regulation--an improvement--but not enough

As a result of changes in requirements of the new Executive order, DOD's Information Security Program Regulation, DOD 5200.1-R, was revised as of August 1, 1982. Of particular concern to us are certain changes to chapter XII, applicable to special access programs. We believe that three provisions of the revised chapter are improvements. First, each DOD component will be required to establish a single point of contact for security control and administration of all special access programs and carve-out contracts. Second, the use of carve-out contracts that do not support properly approved special access programs is prohibited. Third, each component is required to establish a written security plan for each carve-out contract. The Secretaries of the Army, Navy, and Air Force are authorized to approve special access programs and supporting carve-out contracts within their respective services, and the Deputy Under Secretary of Defense for Policy will approve those belonging to other DOD components.

According to the regulation, approval of a special access program will not automatically include related carve-out contracts; additional justification will be needed to establish such contracts. Documentation that supports the establishment of special access programs and carve-out contracts approved by the military services is to be furnished to the Deputy Under Secretary of Defense for Policy.

We believe that there still is one serious omission in the revised regulation. While it provides that special access

programs, with a few exceptions, shall terminate automatically every 5 years unless reestablished in accordance with procedures for establishing new programs, there is no similar provision for carve-out contracts. Since an unknown number of these contracts already exist (and some do not support special access programs), they could be renewed by the military services without the Deputy Under Secretary of Defense for Policy being informed. For example, we noted one large SCI carve-out contract for various studies and tasks that was awarded for a 10-year period. Two other contractors told us that their carve-out contracts were renewed annually simply by an amendment to the contracts. We believe that these examples illustrate the need for better DOD oversight of the establishment and renewal of carve-out contracts.

RECOMMENDATIONS

We recommend that the Secretary of Defense revise the Information Security Program Regulation to require all components to annually (1) inventory and report the status of all carve-out contracts to the Deputy Under Secretary of Defense for Policy and (2) revalidate the need for renewed contracts or contracts that extend for more than 1 year. We further recommend that the Secretary require the Office of Deputy Under Secretary of Defense for Policy to make periodic inspections of components' central offices to evaluate compliance with the regulation.

IMPROVEMENT NEEDED IN IMPLEMENTATION OF UNIFORM SCIF CONSTRUCTION STANDARDS

The SCIFs that we visited appeared to provide more than adequate physical protection for SCI. Although Government-wide SCIF construction standards are supposed to be uniform, we were advised of some inconsistencies in the implementation of the standards which result in increased costs. We were also told that the Government did not make threat analyses prior to the construction of SCIFs or the approval of existing facilities proposed to be used as DOD SCIFs.

Consistency in SCIF construction standards needed

Executive Order 12333 on United States Intelligence Activities, issued December 4, 1981, provides that the Director of Central Intelligence shall ensure the establishment by the intelligence community of common security and access standards for managing and handling foreign intelligence systems, information, and products. According to the order, the intelligence community includes the Central Intelligence Agency, DIA, National Security Agency (NSA), the military services and other offices within DOD involved in

intelligence activities, and several other agencies. These provisions of the December order are identical to those of Executive Order 12036 which was in effect from January 1978 until December 1981. In addition, Executive Order 12036 established a National Foreign Intelligence Board to advise the Director of Central Intelligence on various intelligence matters.

The Board established Government-wide SCIF construction standards which agencies incorporated in their regulations and instructions. The DIA, through its Manual No. 50-3: Physical Security Standards for Sensitive Compartmented Information Facilities, established minimum standards for the construction and protection of DOD SCIFs that are applicable to all DOD components except NSA.

NSA SCIF construction standards are higher and more costly than those prescribed by DIA. One contractor told us that his company had planned to construct a new SCIF for one of the military services at a cost of about \$100,000. Because the company anticipated obtaining an NSA contract, the SCIF was being constructed to NSA standards which were increasing the cost by \$25,000, or about 25 percent, to \$125,000. Two other contractors also commented about the higher NSA standards. Since other DOD components use contractor SCIFs that contain information similar to the level and type of information that NSA keeps in such SCIFs, we believe that the implementation of higher, more costly standards by NSA is questionable.

An NSA official told us that its SCIFs are constructed to standards issued by the Director of Central Intelligence and, in some cases, appeared to be higher than those established by DIA. Since NSA and DIA SCIF construction standards are based on standards established by the National Foreign Intelligence Board, we believe that substantial differences in the standards or their implementation should not be occurring.

Although we did not make a detailed comparison of SCIF construction standards issued by DIA with those of the Director of Central Intelligence (used by NSA), it appears that either the standards or their implementation do not adhere to Executive order requirements for the use of common security standards among agencies in the intelligence community.

Even though the military services were using the same DIA standards, there appeared to be inconsistent implementation as noted in the following example. One contractor told us that one service, using space in a SCIF sponsored by a second service, had said that it would not have approved the SCIF because of the type of window protection used in the SCIF.

Threat analyses should be made

Industry and DOD security personnel told us that DOD did not make threat analyses prior to the approval of existing facilities that were proposed to be used as SCIFs, for the construction of new SCIFs, or for construction of additions to existing SCIFs. There is no specific provision in the DIA manual for such analyses. To ensure adequate protection for SCI and to minimize the high costs of overprotection, we believe that such an analysis should be a prerequisite to the construction and approval of a SCIF.

The SCIF construction standards prescribed by DIA are minimum standards that are intended to protect SCI. Waivers to the standards are occasionally requested by contractors when compliance with the standards is impossible, impractical, or unnecessary. The SCIF sponsors--Army, Navy, or Air Force--review and approve or disapprove the requests. We noted numerous types of SCIFs and security arrangements in our visits to 40 contractors that leads us to believe that DOD threat analyses, prior to construction of the SCIFs, could reduce costs in cases where the SCIF sponsors identify requirements that could be waived without jeopardizing security. For example, should the requirements for a SCIF located in space leased in a building with other private businesses and no guard service be the same as those for a SCIF in a privately owned building with good overall security, including 24 hour guard service?

We believe that the consequences of inconsistent SCIF standards--inadequate security or excessive security and costs--warrant continuing efforts to provide adequate security at minimum costs. With respect to industry SCIFs sponsored by the military services, we believe that greater consistency could be accomplished if one group in DOD, such as DIA, was responsible for (1) conducting threat analyses prior to the construction of new SCIFs, additions to existing SCIFs, or approval of existing facilities proposed as SCIFs, and (2) approving industry SCIFs for DOD use.

RECOMMENDATIONS

We recommend that the Secretary of Defense (1) direct DIA to revise its regulations to require that a threat analysis be made before a SCIF is constructed or altered or an existing facility is approved for use as a SCIF; and (2) make DIA responsible for approving all industry facilities proposed for use as DOD SCIFs.

NEED FOR ONE GROUP IN
DOD TO INSPECT ALL SCIFs
AND SPECIAL ACCESS CONTRACTS

Centralized inspections of SCIFs and special access contracts by one group in DOD could (1) eliminate or substantially reduce the number of carve-out contracts; (2) ensure that all contractor SCIFs and the documents therein are being inspected at least annually; and (3) eliminate or reduce duplicate inspections of the same SCIFs.

Eliminate or reduce the number of carve-out contracts

If DIS was permitted to periodically inspect all SCIFs and most special access contract documents stored therein, most carve-out contracts, by definition, would automatically be eliminated. Elimination of the carve-out status of a contract would not affect its status as a special access contract.

Documents requiring the extra protection afforded by a SCIF could still be stored in the SCIF, and restricted personnel access could still be maintained. A limited number of DIS inspectors could be granted the special access authorizations required for the various special access programs. Many of the SCIFs could be inspected at the same time that DIS inspections are made of contractor facilities under the Defense Industrial Security Program. That means that many SCIFs would be inspected more frequently, and the inspections could be performed at less cost to the Government.

Contractor SCIFs sponsored by DOD components, other than NSA, are required to be inspected annually. (NSA inspects its SCIFs three times a year.) Contractor facilities, other than SCIFs, that store top secret and secret material are inspected by DIS semiannually. Since the purpose of a SCIF is to provide added protection to especially sensitive national security information, more frequent inspections by DIS would be consistent with that purpose.

One of the military services and two other large DOD components use their headquarters staffs to make SCIF inspections. That means that SCIF inspections on the west coast and in other parts of the country require additional travel time and transportation and per diem costs that would not be necessary if DIS, with its 65 offices nationwide (and 175 inspectors), were to make the inspections.

Ensure periodic inspections of all SCIFs and documents

The headquarters office of one of the military services, responsible for administering SCI special access programs and

contracts, did not maintain administrative control over physical inspections of contractor SCIFs. Although the headquarters office conducted inspections of some SCIFs, it relied upon major commands to inspect the balance of the SCIFs sponsored by that service. There was no system for ensuring that the commands were making the required SCIF inspections on an annual basis.

A review of contractor procedures for handling and controlling SCI documents is a required part of the annual physical inspection by the SCIF sponsor. We were told by SCIF sponsors that the inspection also includes a test of the contractor's accountability system for selected documents. However, unless the inspection team is composed of representatives of the components who are tenants, only the contract documents of the SCIF sponsor are likely to be checked against accountability records during the inspection.

The DIA Manual No. 50-5, Volume 1: Sensitive Compartmented Information (SCI) Contractor Administrative Security, contains guidance for contractors to use in protecting SCI. The only requirement in the DIA manual applicable to DOD tenant components appears in a sample memorandum of agreement that establishes areas of responsibility between the SCIF sponsor and tenant. One of the designated responsibilities of the tenant is to perform periodic inspections of its SCI contracts in the SCIF. A specific time frame is not established for such inspections, although a possible assumption is that it is the same as for SCIF sponsors--12 months.

The three military services have not established procedures that require contract monitors to notify their respective headquarters offices that inspections have been made of SCI documents where the services are SCIF tenants. Headquarters officials of two of the services acknowledged that this situation might be a weak link in the DOD system for monitoring SCI documents in industry.

Several contractors told us that contract monitors either had never inspected SCI documents that were in their SCIFs under a tenant arrangement or had done so infrequently. In one case, contract documents had not been inspected by a military tenant for 6 years. Another contractor said that a military tenant had not inspected contract documents for 5 years. A few contractors told us that, to facilitate working with some contracts, documents not requiring special access controls were stored in SCIFs along with documents that required special handling. DOD components inspected the special access documents but not the other group. Since DIS inspectors were not allowed to inspect the SCIFs or their contents, the non-special access documents were not inspected by anyone.

Eliminate or reduce duplicate inspections

Although DOD has made some improvement in reducing duplication of inspections of the same industry SCIF by DOD components, there still is room for more improvement. We were told of one recent incident in which a SCIF inspection by one DOD component was followed several days later by a similar inspection by another DOD component.

One service told us that, in some cases, it did not accept the inspections performed by another DOD component because the inspection reports did not disclose or ensure that thorough inspections had been made. Consequently, the service inspected facilities that had already been inspected.

We believe that centralized inspections of contractor SCIFs and special access contract documents by one group in DOD could eliminate or substantially reduce the number of carve-out contracts and result in improved security assurance at less cost.

Since the purpose of a SCIF is to provide greater protection to SCI, we believe it is vital that all SCIFs and all the classified information therein be inspected at least annually regardless of whether the information belongs to the SCIF sponsor or tenants. Because there have been instances where tenants have not inspected their SCI and other classified documents or access controls, we believe that security assurance could be improved if DIS were to inspect all SCIFs and their contents. In many cases, such inspections could be done concurrently with the periodic inspections that DIS makes of the contractors' facilities and other classified documents. Centrally controlled inspections by DIS would also eliminate or reduce duplicate inspections being made by other DOD components.

RECOMMENDATION

We recommend that the Secretary of Defense make DIS responsible for (1) inspecting all DOD sponsored contractor SCIFs and (2) verifying accountability for all contract documents maintained in those SCIFs and in SCIFs sponsored by other agencies.

IMPROVEMENT NEEDED IN THE ADVANCE
APPROVAL OF SPECIAL ACCESS REQUESTS
THAT REQUIRE SPECIAL
BACKGROUND INVESTIGATIONS

Some contractors, in excess of their specific needs, were submitting requests for special access authorizations

that require special background investigations by DIS. The excess requests were submitted to fill positions in anticipation of new contracts and employee turnover. This practice, which is contrary to DOD instructions, could be eliminated or curtailed by strict enforcement of the requirement for DOD advance approval of contractors' requests for special access authorizations. The successful completion of a special background investigation is a prerequisite for access to all SCI contracts and to many non-SCI special access contracts. The excess requests have increased the DIS workload and contributed to delays in the processing of all requests for investigations.

The DIA Manual No. 50-5, Volume 1, contains a chapter on SCI billets or authorized positions, including procedures for getting SCI access approval of contractor employees who will fill the billets. Generally, when an SCI contract is awarded, the DOD component establishes a specific number of billets which are valid for the duration of the contract. An approved billet (that is vacant or soon will be vacant) should exist before the contractor initiates action to obtain approval of SCI access for an employee. Before submitting a request for a special access authorization to DIS, the contractor is supposed to forward the nomination of a candidate, along with a completed personnel security questionnaire, to the cognizant DOD component for advance approval. After approval, the request is sent to DIS.

There is no DOD requirement that advance approval be obtained for requests for special access authorization needed for access to non-SCI special access contracts.

Contractors were reluctant to admit that they were submitting more requests than they specifically needed. Some said that it was possible to circumvent the system. Two contractors said that they did request a few more special access authorizations than they needed immediately. Both contractors said that the delay by DIS in completing investigations forced them into an untenable situation. If they received a new contract or needed additional employees for an existing contract, they could transfer appropriately cleared employees from other contracts (which would delay that work), hire other contractors' employees who already had special access authorizations (which was costly), or submit requests in anticipation of need.

Some of the contractors that we visited told us that not all DOD components approved their requests before they were sent to DIS. One contractor said that two of the military services were slow in reviewing and approving the contractor's requests. Another contractor told us that one component (not

one of the military services) took 5 to 6 weeks to approve requests.

An official of the DIS office that receives contractors' requests for authorizations and the ensuing investigations told us that as long as a request has an approved program identifier on it they have to assume that it is an approved request. Only one DOD component provides the office with a separate list of approved nominees enabling the office to verify the need for the investigations. We do not feel that a program identifier is sufficient proof that a request for an authorization and investigation has been approved. We believe that the cognizant DOD components should approve and annotate each request before it is sent to DIS.

Our discussions with DOD and contractor officials indicate that it is a pervasive practice for contractors, without the approval of the cognizant DOD components, to request special access authorizations for employees before there is a need for the employees' services on specific contracts. This practice, which is contrary to DOD instructions for access to SCI, causes an unwarranted increase in the DIS workload and delays completion of those investigations for which there is a legitimate need. We believe that DOD should also issue instructions that will require the advance DOD approval of requests for special access authorizations that are needed for employees to work on non-SCI special access contracts.

RECOMMENDATIONS

We recommend that the Secretary of Defense (1) issue instructions that will require advance DOD approval of contractors' requests for special access authorizations for employees who will be working on non-SCI special access contracts; (2) direct DIS to return to contractors any requests for special access authorizations that do not contain the advance approval of the cognizant DOD component; and (3) remind DOD components of their responsibility to review and approve, in a timely manner, contractor nominees for all special access authorizations.

Request for copies of GAO reports should be sent to:

**U.S. General Accounting Office
Document Handling and Information
Services Facility
P.O. Box 6015
Gaithersburg, Md. 20760**

Telephone (202) 275-6241

The first five copies of individual reports are free of charge. Additional copies of bound audit reports are \$3.25 each. Additional copies of unbound report (i.e., letter reports) and most other publications are \$1.00 each. There will be a 25% discount on all orders for 100 or more copies mailed to a single address. Sales orders must be prepaid on a cash, check, or money order basis. Check should be made out to the "Superintendent of Documents".

