United States General Accounting Office 130442

GAO

Report to the Chairman, Subcommittee on Government Information, Justice, and Agriculture,
Committee on Government Operations
House of Representatives

June 1986

DOD TEMPEST PROTECTION

Better Evaluations Needed to Determine Required Countermeasures

RELEASED

GAO/NSIAD-86-132

GAO

United States
General Accounting Office
Washington, D.C. 20548

National Security and
International Affairs Division

B-222962

June 27, 1986

The Honorable Glenn English
Chairman, Subcommittee on Government Information,
Justice, and Agriculture
Committee on Government Operations
House of Representatives

Dear Mr. Chairman:

In response to your September 1984 request, we have reviewed Department of Defense (DOD) and service adherence to national TEMPEST policy. TEMPEST refers to technical investigations and studies of compromising emanations from electronic information-processing equipment. Compromising emanations are unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose classified information. National policy instructs federal agencies to protect classified information against such emanations.

TEMPEST countermeasures—such as metal shielding, special wiring, and special equipment—are costly to implement. Total TEMPEST costs within DOD are unknown; however, they are estimated at hundreds of millions of dollars annually.

Although new procedures for implementing national TEMPEST policy were issued in January 1984, DOD has not issued a corresponding implementing regulation, nor has it issued formal interim instructions. (DOD's current regulation was last updated in 1968) Instead, DOD has issued two policy memorandums. As a result, the military services are interpreting and implementing TEMPEST policy in different ways.

TEMPEST evaluations should be done before TEMPEST countermeasures are implemented or classified information is processed. However, we found that the services sometimes acquire TEMPEST countermeasures without evaluating whether they are needed. This could be wasting money since evaluations often result in the military's or contractors' implementing less costly countermeasures that still meet the national guidance criteria. On the other hand, the military and contractors are sometimes processing classified information without evaluating the risks of compromising emanations; this could be risking the compromise of classified information. We believe that an underlying reason for the services' differing implementation of TEMPEST policy is the lack of formal DOD regulations implementing the January 1984 national policy.

When the services determine that TEMPEST countermeasures are needed at contractor facilities, follow-up inspections are not always conducted to ensure that the countermeasures are implemented correctly. The services say that they have too few trained staff to perform such inspections. Furthermore, some service officials told us that they rely on the Defense Investigative Service (DIS) for TEMPEST evaluations. They said that they believe that DIS is responsible not only for making compliance inspections but also for assessing the degree of protection needed. However, while DIS is responsible for investigating contractor compliance on a wide range of security measures, including TEMPEST, it cannot disapprove a system that does not meet TEMPEST requirements but can only bring its concerns to the attention of the contracting officer. As a result, we found that some contractors were processing classified information without ever having an evaluation done of TEMPEST countermeasures that may be needed.

DIS officials told us that their inspectors lack the trained expertise to fully do TEMPEST compliance inspections. Also, they do not have adequate resources to do evaluations to assess what countermeasures are needed at contractor facilities.

A contractor doing work for more than one service may have differing TEMPEST requirements imposed by each service. Consolidating TEMPEST evaluation and inspection resources in one office may be a more effective way to oversee industry compliance with TEMPEST requirements. Because DIS already has a responsibility to review contractor security measures, it would seem a likely office for such responsibility. This would require additional training for its inspectors and possibly more staff resources.

Recommendations

We are recommending that the Secretary of Defense

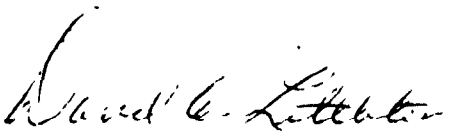
- promptly implement new security policy—on an interim basis if necessary—and ensure that the services promulgate implementing instructions to the field in a timely manner,
- require DOD components to conduct a TEMPEST evaluation before TEMPEST countermeasures are implemented, and
- consider assigning to the Defense Investigative Service, or some other DOD component, the responsibility for ensuring that industry is effectively implementing TEMPEST countermeasures.

As you requested, we did not ask for agency comments, but we did discuss our findings informally with DOD officials who generally agreed with our recommendations. However, they did not agree on where within DOD the central responsibility for overseeing industry TEMPEST countermeasures should be placed. In addition, DOD officials told us that, while problems still exist in the TEMPEST program, many improvements are being made.

Certain information that would have been helpful in better understanding this report on TEMPEST is classified and was not included because your office requested an unclassified report. Still, the National Security Agency (NSA) believes that, although not technically classified, this report contains "extremely sensitive information, which, if made public, would be detrimental to the United States Government TEMPEST Program." NSA, however, declined to place a security classification on the information. Moreover, the information NSA identified to us as sensitive can be obtained from readily available unclassified sources. We thus have no basis for restricting distribution of this report

We are sending copies of this report to the Chairmen, House Committee on Government Operations, the Senate Committee on Governmental Affairs, and the Senate and House Committees on Armed Services and Appropriations; the Secretaries of Defense, the Army, the Navy, and the Air Force; and the Director of the Office of Management and Budget. Copies will be made available to other interested parties on request.

Sincerely yours,



Frank C. Conahan
Director

DOD and Service Implementation of TEMPEST Policy

Current national TEMPEST policy is embodied in National Communications Security Committee Directive 4, "National Policy on Control of Compromising Emanations," dated January 16, 1981, which instructs federal agencies to protect classified information against compromising emanations. The National Communications Security Instruction (NACSI) 5004 (classified Secret), published in January 1984, provides procedures for departments and agencies to use in determining the countermeasures needed for equipment and facilities which process national security information in the United States.

National Security Decision Directive 145, dated September 17, 1984, designates the National Security Agency (NSA) as the focal point and national manager for the security of government telecommunications and automated information systems NSA is authorized to review and approve all standards, techniques, systems, and equipment for automated information systems security, including TEMPEST. In this role, NSA makes recommendations to the National Telecommunications and Information Systems Security Committee for changes in TEMPEST policies and guidance.

Slow Implementation of TEMPEST Policy in DOD

NACSI 5004 was issued in January 1984 but, as of May 1986, DOD had not issued any formal policy directives or interim instructions implementing NACSI 5004. (DOD last updated its TEMPEST regulation in 1968.) In December 1984 and May 1985, the Deputy Undersecretary of Defense for Policy issued policy memorandums specifically exempting systems from TEMPEST countermeasures if the systems do not process classified information higher than the Confidential level, and a "clear and compelling requirement" for these countermeasures is needed at the Secret level. The 1984 memorandum established this policy for use at defense-contractor facilities. The 1985 memorandum extended the policy to the military services The services, however, have not consistently implemented the intent of NACSI 5004 or the memorandums.

The Air Force notified field activities in September 1984 that NACSI 5004 was available and that it could help in determining required TEMPEST countermeasures. However, the Air Force has a decentralized TEMPEST program, which leaves the use of NACSI 5004 and decisions about protective measures to the discretion of each command. Two of the ten TEMPEST officers we visited had not obtained copies of NACSI 5004 even though it had been issued over a year earlier. One of the two was requiring TEMPEST-approved equipment for all classified processing. Four of the eight who had NACSI 5004 available were continuing to follow older,

more stringent guidance, which could be resulting in unnecessary TEMPEST protection. The Air Force expects its implementing regulation to be available in June 1986.

The Navy, which until recently had a centralized TEMPEST program, has not made NACSI 5004 available to its field commands. The Navy has drafted a new TEMPEST regulation which incorporates the guidance of NACSI 5004 except that the Navy believes that systems processing Confidential information should still be evaluated for the need for TEMPEST countermeasures. This draft was sent to field commands during September 1985, in anticipation of its official release, with the intent that the TEMPEST officers use the regulation immediately. (The Navy is not sure when the final regulation will be issued.) The proposed regulation allows field TEMPEST officers to perform evaluations similar to those in NACSI 5004 and determine the most appropriate TEMPEST countermeasure for a given situation.

The Army has not yet formally made NACSI 5004 available to its field commands. However, it did issue its implementing instruction on January 31, 1986.

Evaluations Often Not Performed Before Deciding on TEMPEST Countermeasures

Although the regulations of major DOD components require an evaluation to determine whether and what TEMPEST countermeasures are needed, these evaluations were often not made. The absence of the evaluations has, in some cases, caused DOD components to spend more money than necessary to protect classified information The lack of evaluations could also result in insufficient protection being given to classified information.

The practice followed at many of the service locations has been to require TEMPEST-approved equipment in all cases in which an activity needs to process classified information, even though a determination has not been made that such countermeasures are actually necessary. For example, at four Air Force locations we visited, TEMPEST officers were requiring TEMPEST-approved equipment for all classified data processing, without making a prior evaluation of need. We also found that one Navy activity installed TEMPEST equipment before submitting data—about the information being processed and the countermeasures being taken— for a TEMPEST evaluation by the responsible Navy command. This approach prevents an evaluation of need for TEMPEST countermeasures before electronic information-processing equipment is acquired

Costly TEMPEST Countermeasures

TEMPEST countermeasures, such as metal shielding, special wiring, and special equipment, are costly to implement The cost of providing TEMPEST protection to equipment varies for many reasons, including type of equipment and number of units purchased. The Air Force estimates that TEMPEST protection adds about 25 percent to the cost of equipment. Industry sources indicate that TEMPEST-protected equipment can cost more than twice as much as unprotected equipment.

Although total TEMPEST costs are not a separate budget line item and therefore not readily determined, there are some indications of their magnitude. A November 19, 1985, report of the DOD Security Review Commission states that the total costs of TEMPEST countermeasures are estimated to be hundreds of millions of dollars annually. DOD has authorized over 12,000 contractor facilities to handle classified materials. About 2,000 of these facilities have about 12,600 automatic data-processing systems authorized to process classified information.

Possible Cost Savings by Making Evaluations

Many have recognized the large cost savings possible through the use of NACSI 5004 evaluations before TEMPEST countermeasures are implemented. For example, the report of the DOD Security Review Commission stated that substantial costs could be avoided by using NACSI 5004. The report, however, did not make any specific recommendations concerning TEMPEST.

An Army field TEMPEST officer wrote the following to a headquarters command, in a message dated April 8, 1985:

"On recent test/inspection trips within this unit's AOR [Area of Responsibility], confusion was found among TEMPEST Security Offices (TSO) in regards to the application of TEMPEST countermeasures. Despite [another command's] attempt in keeping Army field elements from becoming aware of NACSI 5004, TSO's are not only aware of it but are using it.... The application of NACSI 5004 will save supported commands money that would not be saved using existing TEMPEST policy and guidance.... This office finds NACSI 5004 an excellent money-saving document."

In June 1985, the headquarters command issued a service-wide message that NACSI 5004 was being incorporated into the Army TEMPEST regulation and instruction but that NACSI 5004 was still not to be distributed directly to Army commands. Army officials told us that they believe that NACSI 5004 is procedural, not directive, in nature and think that it is too general for use in the field.

An Air Force audit report, dated September 4, 1985, entitled Management of the Air Force TEMPEST Program, found that, at two bases, approximately $126,000 was spent to purchase word processors with unneeded TEMPEST enhancements because the need for such equipment had not been adequately evaluated. Air Force management agreed with the report findings and planned to implement the report recommendations through changes in the appropriate regulations.

We found the following examples of money being saved after the use of an NACSI 5004 evaluation:

- A contractor had originally planned to build two shielded enclosures to support contract requirements. After doing an evaluation, however, the contractor was able to use less costly but still effective countermeasures, resulting in an estimated savings of $800,000.
- Another contractor had been directed to provide TEMPEST protection. After an evaluation, requested by the contractor, the TEMPEST requirements were reduced and $125,000 was saved.
- One Air Force program office instructed a contractor to build a shielded enclosure costing an estimated $500,000. When the contractor objected, the program office contacted its command's TEMPEST liaison for assistance. After performing an evaluation, the liaison determined that less expensive TEMPEST countermeasures would provide adequate protection for about $90,000.

Contractors Not Always Required to Use TEMPEST Countermeasures

According to the DOD Industrial Security Regulation dated December 1985, TEMPEST countermeasures must be used at contractor plants only if the DOD agency involved specifically requires such protection in the contract. The regulation makes the contracting officer responsible for ensuring that necessary TEMPEST countermeasures are included in classified contracts when a need has been identified. It gives DIS, as the cognizant security office for most contractors, the responsibility for inspecting a contractor's facility for the TEMPEST provisions of contracts, but not the authority to disapprove a system processing classified information that does not comply with national policies for the control of compromising emanations. If DIS believes that TEMPEST countermeasures should be included in a contract, DIS is to alert the appropriate contracting officer.

Not all commands that award contracts, however, are aware of this assignment of responsibility and assume that DIS is responsible for not

only inspecting but also for setting TEMPEST requirements for contractors. Consequently, in many instances, service personnel do not evaluate the need for TEMPEST countermeasures before issuing contracts involving the processing of classified information, and they do not require contractors to use the necessary countermeasures.

For example, the September 4, 1985, Air Force audit report on the management of the Air Force's TEMPEST program stated that, of the 214 contractor systems reviewed, the majority were processing classified information even though the required TEMPEST inspections had not been performed. Consequently, the report noted, there was no assurance that the classified information was being adequately safeguarded and was not being compromised.

We found that one Navy command had not required its contractor at a nearby location to use TEMPEST countermeasures when processing classified information, even though the Navy had thought such countermeasures necessary to use when it had processed similar information. The program office did not require TEMPEST protection nor did it evaluate whether such protection was needed at the contractor's facility because it assumed that DIS was responsible for such matters. At another Navy command, the Station TEMPEST Officer told us that he reviewed all contracts to make sure that adequate security requirements, such as physical and personnel security controls, were included in contract documentation, but that he never reviewed the contracts to ensure that TEMPEST needs were evaluated. This TEMPEST officer also believed that DIS was responsible for evaluating contractors' needs for TEMPEST countermeasures.

The Industrial Security Manual for Safeguarding Classified Information, issued by DIS, does establish special security measures (such as administrative and personnel security controls) for the safeguarding of classified information being handled by automatic data processing and word processing systems at the facilities of DOD contractors having classified information. The manual is silent on the subject of TEMPEST, however, a proposed change to the manual was circulated for comment at the end of March 1986. Although the change adds definitions and some guidance to contractors concerning TEMPEST, it does not identify DIS as the agency responsible for monitoring compliance with TEMPEST requirements at contractor facilities, as required by the Industrial Security Regulation.

Lack of Follow-Up on Contractor Use of TEMPEST Countermeasures

Even when the services require that their contractors use TEMPEST countermeasures, they usually do not make follow-up inspections to ensure that contractors actually do so. The services told us that they lack sufficient resources to provide timely inspection and testing of their own facilities (except for emergency situations). Five TEMPEST officers we visited said that they are able to respond to few contractor requests for TEMPEST inspections

Even though most of the contracts that we found with TEMPEST requirements originated at Air Force program offices, Air Force follow-up at contractors is limited. One Air Force TEMPEST officer believes that contracting officers lack sufficient trained staff to inspect all contractor facilities where TEMPEST is a requirement. Five contractors we interviewed commented that they had never had any representatives from the Air Force inspect their TEMPEST installations.

The Navy does not make routine follow-up inspections, but it does perform some. According to an Army TEMPEST Team Chief, the Army does a limited number of follow-up inspections at contractor facilities, depending on staff availability. Without inspections, the services cannot be sure that required TEMPEST countermeasures are implemented correctly, if at all.

As stated earlier, DIS has an inspection responsibility for TEMPEST However, DIS officials told us that their personnel lack the technical expertise, in most cases, to perform TEMPEST inspections. Instead, when inspectors visit a contractor facility, they often check only to see whether the contractor has prepared a TEMPEST-implementation plan, and do not evaluate whether or how the TEMPEST requirement is met.

During our review, we found two contractors not complying with the TEMPEST requirements of the services for whom they were working One contractor was processing classified information without TEMPEST evaluations being performed and without TEMPEST precautions for any contracts (including the six we reviewed). The contractor believed that the government should be paying the cost of providing the information needed for an evaluation for TEMPEST and did not intend to implement the TEMPEST countermeasures until the government did pay. When this situation was brought to the attention of the two services involved, both agreed that problems in monitoring TEMPEST compliance existed Both services were relying on DIS to ensure compliance with their TEMPEST requirements However, as previously noted, DIS does not verify TEMPEST compliance in its inspections of contractor facilities.

Another contractor had also not implemented TEMPEST countermeasures because the contractor believed that the contracting agency should bear the costs of the countermeasures This contractor subsequently contracted for a commercial evaluation of its facility, which recommended changes to bring the facility into full TEMPEST compliance The contractor is awaiting estimates for complying with the recommendations and, in the meantime, has permission from the service involved to continue processing classified information

For the most part, the services believe that TEMPEST costs are the responsibility of the contractors Eventually, however, TEMPEST costs are passed back to the government, if not by direct charges then through overhead charges spread over many contracts

Conclusions

Implementation of NACSI 5004 and other recent guidance has been slow and has differed among the services. We found that, for more than a year after the issuance of NACSI 5004 in January 1984, the services all continued to follow their older internal TEMPEST guidance. As of May 1986, DOD had not issued a new regulation implementing NACSI 5004.

The Army issued a change to its regulation on January 31, 1986, and the Air Force expects its revised regulation to be issued in June 1986. The Navy is unsure when its new regulation will be issued In some of the cases we examined, the military services spent more money on TEMPEST protection than they would have if they had performed a NACSI 5004 evaluation before installing TEMPEST countermeasures The services' continued delay in implementing the newer policies and, instead, using older and more stringent TEMPEST guidance can lead to further unnecessary expenditures.

In addition, DOD personnel responsible for ensuring that contractors protect classified information from compromising emanations are, in many instances, unaware of the extent of their responsibility and assume that DIS is responsible for setting TEMPEST requirements for contractors and then inspecting for compliance with those requirements Current regulations require the DOD agency involved to specify the TEMPEST countermeasures needed at a contractor facility. Further, even though DIS has an inspection responsibility for TEMPEST compliance, it does not currently have the technical expertise to perform those investigations, nor is it responsible for considering TEMPEST requirements when it approves a contractor system for processing classified information DOD, by not

specifying, tracking, or following up on contractual TEMPEST requirements, is not ensuring that classified information at contractor locations is receiving adequate protection.

We believe that the imposition of TEMPEST countermeasures on industry should be controlled from a central point within DOD. Without this central control, contractors can be subject to varying TEMPEST requirements placed on them by the services, and duplicative resources within the services are required to identify and evaluate contractor systems that need protection. DIS is a likely office for the central role because it is already responsible for the administration of the DOD Industrial Security Program. (The DOD Industrial Security Program was created to ensure maximum uniformity and effectiveness in the safeguarding of classified information in industry.)

Recommendations

We are making the following recommendations to the Secretary of Defense:

To minimize delay in implementing national security policy, we recommend that the Secretary of Defense promptly implement new security policy—on an interim basis if necessary—and ensure that the services promulgate implementing instructions to the field in a timely manner.

To minimize unnecessary TEMPEST-related expenditures, we recommend that the Secretary of Defense require all DOD components to conduct a TEMPEST evaluation before implementing TEMPEST countermeasures. Such evaluations are also needed to ensure proper protection of classified information.

To reduce varying requirements placed on industry and duplicative efforts on the part of the services, we recommend that the Secretary of Defense consider assigning to the Defense Investigative Service, or some other DOD component, the responsibility for ensuring that TEMPEST countermeasures are effectively implemented within industry. Implementation of this recommendation may require additional training for the designated component's staff.

Objectives, Scope, and Methodology

As agreed with your office, our objectives were to evaluate DOD's and the military services' compliance with national TEMPEST policy and to determine how they make sure that the TEMPEST countermeasures taken were necessary and the most cost-effective ones. (We did not examine

the use of these countermeasures for the protection of sensitive compartmented information or at overseas locations.)

We visited 23 DOD offices and installations and 23 contractor facilities in 12 states and the District of Columbia. At these locations, we interviewed DOD and contractor personnel and reviewed pertinent regulations and instructions, contract security specifications, and inspection reports. We selected contractors and DOD components based on (1) their size and known TEMPEST activity, (2) contract security specifications, and (3) industry complaints.

Our review was made in accordance with generally accepted government auditing standards.

Requests for copies of GAO reports should be sent to.

U.S. General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877

Telephone 202-275-6241

The first five copies of each report are free. Additional copies are $2.00 each.

There is a 25% discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.

United States
General Accounting Office
Washington, D.C. 20548

Official Business
Penalty for Private Use $300

Address Correction Requested

First-Class Mail
Postage & Fees Paid
GAO
Permit No. G100