

7040

March 1978

REPORT BY THE U.S.

General Accounting Office



LM106473

VA's New Computer System Has Potential To Protect Privacy Of Individuals Claiming Benefits

VA's proposed Target System, a computer system intended to modernize benefit claims service to veterans, can provide a high level of protection of personal information on benefit claimants if the system is properly designed and implemented.

VA recognizes that it must assess risks of privacy violations in Target more thoroughly to make sure it has selected adequate yet cost-effective safeguards to protect personal information.

GAO recommends that VA adopt standard identification procedures to prevent inadvertent disclosure of personal information to unauthorized parties when Target is operational. GAO also recommends that VA's Inspector General participate in Target's risk assessment to make sure that financial data as well as personal data is also protected.



HRD-78-135
JULY 17, 1978

U27040



UNITED STATES GENERAL ACCOUNTING OFFICE

WASHINGTON, D.C. 20548

HUMAN RESOURCES
DIVISION

B-133044

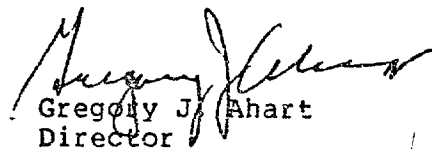
The Honorable John E. Moss
The Honorable Charles Rose
House of Representatives

This is our report on our review of the Veterans Administration's (VA's) efforts to protect personal information on benefit claimants in the Target System.

The report contains recommendations to the Administrator of Veterans Affairs on page 22. As you know, section 236 of the Legislative Reorganization Act of 1970 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. We will be in touch with your offices in the near future to arrange for release of the report so that the requirements of section 236 can be set in motion.

As arranged with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after the date of the report. At that time we will send copies to interested parties and make copies available upon request.

At your request we did not obtain written agency comments. However, the matters covered in the report were discussed with officials of VA's General Counsel, Departments of Data Management and Veterans Benefits, and Office of Inspector General, and their comments are incorporated where appropriate.


Gregory J. Ahart
Director

D I G E S T

The Veterans Administration (VA) is developing a computer system, known as the Target System, intended to modernize benefit claims service to veterans. It will provide immediate access to information concerning claims, status and amount of award checks, and information in the automated master records. Information will be transmitted by communications lines between five computer centers and 2,500 terminals located in VA installations throughout the country.

VA realizes the need for privacy protection and has developed safeguard features in Target's pilot operation for use in the new system. But because the system is not operating yet, GAO cannot make a complete evaluation of Target's ability to protect personal information.

GAO noted in its observation of pilot activities one potential trouble spot which suggests the need for VA to establish standard operating procedures for identifying telephone requestors of information to prevent inadvertent disclosure of information to unauthorized parties. (See ch. 3.)

VA needs to more thoroughly assess risks of privacy violations in the total Target System environment to provide assurance that it has selected adequate yet cost-effective safeguards to protect personal information. VA recognizes this need and plans to perform a risk assessment before Target becomes operational. (See ch. 3.)

VA's Office of Inspector General should participate in the risk assessment; the system disburses billions of dollars annually and an assessment should analyze

risks not only to personal data but to financial data as well. Such participation by the Office of Inspector General can help make sure that adequate controls are established in the system design so that costly changes will be avoided after the system is operational. (See ch. 4.)

VA does not plan to use Target to collect more information on benefit recipients than that maintained in the current system, but its capabilities for reporting on these individuals could be considerably more sophisticated when the system is fully developed. If this happens VA may need to tell the public more specifically what information about individuals is being released, and to whom, to keep the public fully informed. (See ch. 4.)

The Administrator of Veterans Affairs should direct the Office of Inspector General to participate in Target's risk assessment. The Administrator should also direct VA's Department of Veterans Benefits to establish standard procedures for identifying telephone requestors before Target is carried out. This could prevent inadvertent disclosure of personal information to unauthorized parties. (See ch. 5.)

C o n t e n t s

	<u>Page</u>
DIGEST	i
CHAPTER	
1 INTRODUCTION	1
Administration of compensation, pension, and education benefits and services	1
The present benefits delivery system	1
Target System	2
The Privacy Act of 1974	2
Federal Information Network (FEDNET)	3
Scope of review	4
2 THE TARGET SYSTEM	5
Pilot program	7
Target's implementation schedule	7
Personnel information in the Target System	7
Access to and use of information in the CP&E records	8
3 VA IS SENSITIVE TO THE NEED TO SAFEGUARD PERSONAL INFORMATION BUT MUST ASSESS RISKS TO TARGET MORE THOROUGHLY	10
Early consideration of the need for privacy protection features in Target	11
Safeguards in the pilot program	11
Additional protection features planned for Target	13
Training on privacy and security to VA personnel	13
A potential weakspot should be strengthened in Target	14
Efforts to determine the likelihood and cost of external intrusion	14
Need for a risk assessment	15
Need for participation by Office of Inspector General	16
4 TARGET IMPACT ON THE COLLECTION AND TRANSFER OF PERSONAL INFORMATION	18
Collection of information in Target	18
Target's reporting capability	19

5	CONCLUSIONS AND RECOMMENDATIONS	21
	Conclusions	21
	Recommendations to the Administrator of Veterans Affairs	22

APPENDIX

I	Routine uses of Target System records published in the Federal Register September 27, 1977	23
II	Principal VA officials responsible for administering activities discussed in this report	29

ABBREVIATIONS

BIRLS	Beneficiary Identification and Records Locator System
C&P	compensation and pension
CP&E	compensation, pension, and education
FEDNET	Federal Information Network
GAO	General Accounting Office
OMB	Office of Management and Budget
SSA	Social Security Administration
SSI	Supplemental Security Income
VA	Veterans Administration

CHAPTER 1

INTRODUCTION

In response to a request from Congressmen John E. Moss and Charles Rose and interest expressed by several congressional committees, we reviewed the Veterans Administration's (VA's) proposed Target System--a computer system intended to modernize VA's benefit claims processing. We have issued three prior reports on various aspects of our review. 1/ This report examines VA's efforts to provide in Target appropriate technical, administrative, and physical safeguards on benefit claimant information as required by the Privacy Act of 1974 (Public Law 93-579, approved December 31, 1974).

ADMINISTRATION OF COMPENSATION, PENSION, AND EDUCATION BENEFITS AND SERVICES

VA's Department of Veterans Benefits administers non-medical benefits and services through 59 major field stations (58 regional offices and a records processing center) within and outside the continental United States. These benefits and services include compensation for service-connected disabilities; pension for aged, needy, and unemployable veterans; vocational rehabilitation, education, and training assistance; and information and assistance through personal contact. In fiscal year 1977, VA paid about \$9 billion in compensation and pension benefits to 4.9 million veterans and survivors, and about \$3.7 billion in education and training benefits to 2.1 million veterans.

THE PRESENT BENEFITS DELIVERY SYSTEM

The present compensation, pension, and education (CP&E) delivery system was designed and installed in the late 1950s. It is primarily a manual system; only the claims

1/"Review of VA Interim Computer Procurement" (MWD-76-132, June 1, 1976).

"VA Justification for Establishing Four Regional Computer Centers for its Proposed Target System" (HRD-76-145, July 13, 1976).

"Veterans Administration Justification of Costs and Benefits of Proposed Computer System (Target)" (HRD-77-98, July 20, 1977).

payment process is automated. Claims processing and financial activities are performed in all regional offices. These activities include awarding or disallowing claims for benefits; interacting with veterans and beneficiaries; and maintaining the claim folders of veterans and beneficiaries. The regional offices prepare input for a computer center in Hines, Illinois; accumulate the input into batches; and send it to the computer center, generally by mail. At the computer center these transactions are written on magnetic tape and processed sequentially through a series of computer cycles to (1) update CP&E master files, (2) generate payment notices to the Treasury Department, which prints benefit checks, (3) generate various operational and management reports, and (4) perform various accounting functions.

VA characterizes the system as technically limited, labor intensive, and paperwork bound and has proposed the new Target System to improve efficiency and take advantage of new automatic data processing technology.

TARGET SYSTEM

The new computer system being developed by VA is intended to modernize VA's benefit claims-processing system and improve services to veterans.

Benefits expected by VA from the new system include much faster development of claims, more timely delivery of initial benefit checks to veterans, faster responses to veterans' inquiries, and major savings from workload reductions in the regional offices as a result of more efficient procedures and workflow.

According to March 1978 VA estimates, total one-time development costs of the Target System, including the acquisition of data processing and telecommunications equipment, will be about \$81.4 million. Recurring annual operating costs of the system are estimated at \$13.5 million.

THE PRIVACY ACT OF 1974

The Congress passed the Privacy Act of 1974 (5 U.S.C. 552a et. seq.) to assure that personal information about individuals collected by Federal agencies be limited to what is legally authorized and necessary and that it be maintained in a manner which prevents misuse of such information. The act requires Federal agencies to establish appropriate administrative, technological, and physical

safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is obtained.

The Congress gave particular attention to its concern over the increasing use of computers by Federal agencies in the collection and dissemination of information by citing the following in section 2(a)(2) of the act:

"the increasing use of computers and sophisticated information technology, while essential to efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information."

FEDERAL INFORMATION NETWORK (FEDNET)

Indicative of this concern expressed by the Congress in the Privacy Act was its reaction to a proposed joint procurement initiated by the Department of Agriculture and General Services Administration in 1974 for a computer system and an associated telecommunications network, commonly known as FEDNET. Members of Congress expressed concern that FEDNET could be expanded to link all computers in the Government posing a serious threat to the privacy of individuals. As a result, the scope of the project was reduced in July 1974 by canceling the telecommunications network and General Services Administration's participation in the project. Agriculture canceled its procurement action in October 1975. 1/

The Target System differs significantly from FEDNET in that there will be no direct linkage or sharing of equipment with other Government agencies or outside organizations.

1/"Improved Planning--A Must Before A Department-wide Automatic Data Processing System Is Acquired For The Department Of Agriculture" (LCD-75-108, June 3, 1975).

"Challenges Of Protecting Personal Information In An Expanding Federal Computer Network Environment" (LCD-76-102, Apr. 28, 1978).

SCOPE OF REVIEW

We reviewed the requests for proposals for the Target System processing equipment and terminals and associated telecommunications equipment supporting the Target network. We also reviewed other available documentation relating to systems design and plans for Target. We interviewed VA personnel and observed pilot operations at the VA central office, Philadelphia and Baltimore regional offices, and the Hines, Illinois and Philadelphia computer centers. We also interviewed officials of the Office of Management and Budget (OMB), National Bureau of Standards, and the Privacy Protection Study Commission. ^{1/} Because the pilot operation of Target was still in the development stage at the time of our review, and new construction and equipment is planned for Target, we did not test the adequacy of the safeguards employed at the regional offices and the computer centers.

^{1/}The Privacy Protection Study Commission was established by the Privacy Act and was given the broad mandate to investigate the personal data recordkeeping practices of governmental, regional, and private organizations and to recommend to the President and the Congress the extent, if any, to which the principles and requirements of the act should be applied to them.

CHAPTER 2

THE TARGET SYSTEM

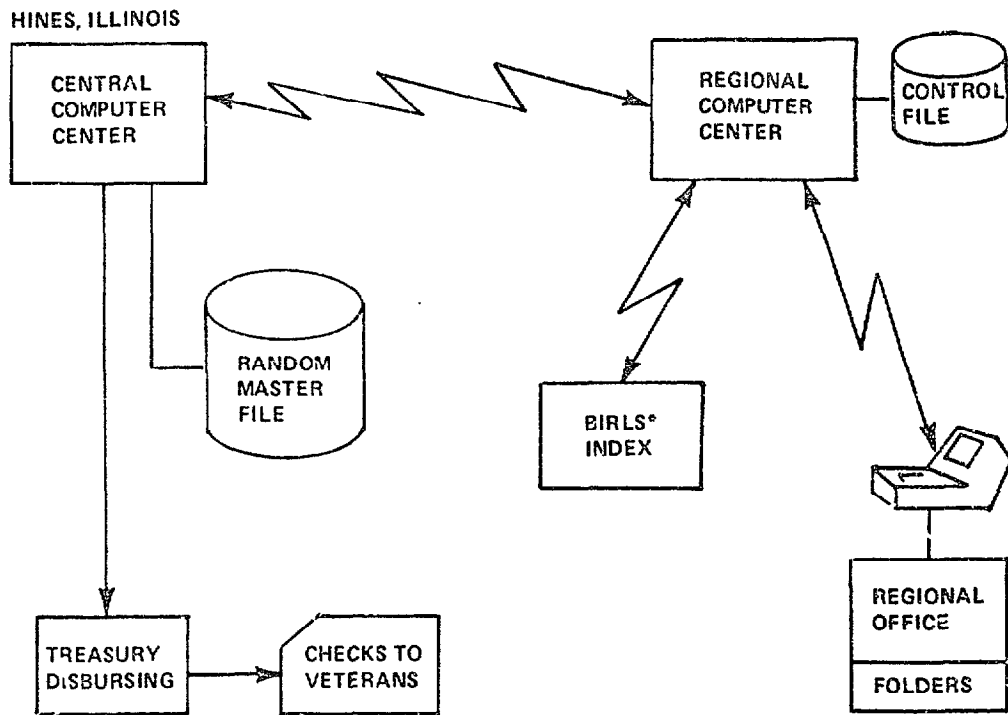
The Target System will use computers in three regional computer centers to provide data entry and automated claims processing capabilities to the VA regional offices. The system will have a central computer facility--Target Central System--for maintenance of master records, centralized reporting and accounting functions, and generation of payment notices to the Treasury Department, which prints the benefit checks. The key operational features of the Target System stated by VA are:

- Computerized processing and control of claims in the regional offices, including automatic calculation of benefit awards, control of pending claims, and workload reporting.
- Immediate response to veteran inquiries concerning (1) status of claims in process, (2) status and amount of award checks, and (3) information in the master record.
- Automated printing of awards, acknowledgements, and other routine letters.
- Ready access to information for reporting.

Terminals, installed in 56 of the 58 regional offices and the records processing center, will be connected to computers in the three regional centers by telecommunications lines. Input data will be transmitted from the regional offices to the regional computers, each of which will maintain on-line work-in-process control files which will be updated automatically as a byproduct of claims processing. The regional offices will be able to obtain from the terminals (1) information concerning pending claims from the regional computer center files and (2) information from the master files at the central computer facility through the regional computer centers. In addition, the regional computer centers will link the regional offices to a claimant locator system at Austin, Texas.

The following chart depicts the operational features of the Target System:

THE TARGET SYSTEM



● 3 REGIONAL COMPUTER CENTERS

● EACH REGIONAL COMPUTER CENTER SUPPORTS UP TO 20 REGIONAL OFFICES AND IS LINKED TO THE REGIONAL OFFICES, BIRLS INDEX, AND CENTRAL COMPUTER CENTER BY TELECOMMUNICATIONS LINES.

**BIRLS (BENEFICIARY IDENTIFICATION AND RECORDS LOCATOR SYSTEM) IS A COMPUTERIZED CLAIMANT LOCATOR SYSTEM.*

PILOT PROGRAM

In September 1974 VA began a pilot test of the Target System processing concepts in Philadelphia and Baltimore. Terminals in selected units of the Philadelphia and Baltimore regional offices were linked with a data processing center in Philadelphia, which serves as a regional computer center. The Philadelphia center is also linked with the computerized claimant locator system in Austin and the centralized master files of the benefit claims system at Hines. In the summer of 1975 the pilot test was expanded to three other regional offices--in New York; Washington, D.C.; and Los Angeles. In November 1976 the pilot test was again expanded to place the entire Philadelphia regional office operation under pilot operating conditions.

TARGET'S IMPLEMENTATION SCHEDULE

The General Services Administration awarded a contract in October 1977 for automatic data processing equipment in VA computer centers, terminal equipment in the regional offices, and supporting software and services.

VA had installed the first Target computers at the central facility and at the first of three regional centers in May 1978. VA planned to complete installation of terminals in regional offices supported by the regional center in June 1978. VA plans to begin operations at the computer centers and the first regional office in August 1978 and at the remaining offices supported by the regional center by October 1978.

The Target System will be implemented in phases to offer VA regional offices sufficient time to adjust to the new processing environment. In August 1978 VA plans to (1) implement the capability to inquire through the display terminals as to the status of claimants' master records and location of claims folders, (2) make certain changes to these records through terminals, such as changes of names and addresses and statistical corrections, and (3) stop, suspend, and resume payments to beneficiaries via the terminals. In February 1979 VA plans to implement the automated claims processing capabilities of Target.

PERSONAL INFORMATION IN THE TARGET SYSTEM

The Target System, like the current CP&E system, will maintain records on veterans, surviving spouses, children, and dependent parents in connection with claims for

service-connected and non-service-connected disability and death benefits and education benefits administered by VA. The types of information contained in these records include military service and active duty separation; medical records related to treatment in service; medical information from VA and private hospitals and doctors; applications for compensation, pension, education, and rehabilitation benefits and training; information relating to dependency, income, education, occupation, marital status, and educational status relative to VA benefits; payment data; counseling and rehabilitation records; and claimant and payee names and addresses.

Under the current CP&E system all data gathered on claimants are contained in claims folders located and maintained manually in the regional offices or in the VA records processing center in St. Louis. Claims folders are needed for processing the claims and for practically all inquiries concerning the claims. Part of the information in the claims folders is on computerized master records and is accessible for inquiry, but it generally takes about 3 weeks to obtain a computer printout of the data.

Under the Target System a wide variety of abstracted information concerning the basis for the claim, the status of the claim, and the benefits received will be on automated records accessible almost immediately through display of the information on video display screens or printed from terminals located in the VA regional offices. This immediate access to the automated records is intended to reduce the need for reliance on the claims folders for processing claims and responding to inquiries.

ACCESS TO AND USE OF INFORMATION IN THE CP&E RECORDS

The only persons who can access CP&E records routinely are VA employees, principally those in two major divisions in the VA regional offices. These divisions include the Adjudication Division, where all claims processing functions, including records management, are accomplished; and the Veterans Services Division, where personal contact is made with claimants for providing counseling services and information.

VA also permits access to information to people with personal involvement in the claims or legal authority. For VA, those personally involved include veterans and other persons on whom CP&E records are maintained. They include dependent children, widows, widowers, and parents

1/Section 3(b) of the Privacy Act does not permit disclosure of records of individuals to whom the records pertain to any person or agency without the prior written consent of the individual unless the disclosure of that record would be under 1 of 11 exceptions permitted by the act. One of these exceptions is a routine use (a use which is compatible with the purpose for which the information was collected). The routine uses proposed for Target are shown in appendix I.

When information is requested by individuals or organizations which do not have representational authority, and the request does not constitute a routine use 1/, the information ordinarily will not be released without prior written consent of the veteran or individual on whom the record is maintained.

Persons with legal authority include authorized third parties, such as fiduciaries, guardians, and other agents with powers of attorney. The large majority of authorized third parties are representatives of veterans' service organizations who are designated by such organizations to represent claimants with whom powers of attorney have been executed. Service organization representatives must be approved by VA. Before access to a record can be given to a third party, the record must contain documentation that a valid arrangement exists which permits a third party to act in behalf of the veteran or other individual on whom the record is maintained.

claiming or receiving C&P benefits relating to living, deceased, and/or disabled veterans. Such individuals generally can have access to their records for review. However, the records must be reviewed at a VA office in the presence of a "A employee in order to maintain record integrity.

Because Target is still in the development stage, participation by the Office of Inspector General can help

VA's Office of Inspector General had no plans to participate in the risk assessment. We believe that such participation is essential because Target is a payment system from which billions of dollars are disbursed annually, and the risk assessment should analyze risks not only to personal data but to financial data as well. Most of the safeguards for protecting personal data also provide protection to other valuable data.

Efforts to date by VA to establish appropriate safeguards for Target have been piecemeal and VA needs to more thoroughly assess risks of privacy violation in the total system environment to provide assurance that it has selected adequate yet cost-effective safeguards to protect personal information. VA recognizes this need and has plans to perform a risk assessment before the start of Target operation.

We noted one potential trouble spot in our observation of pilot activities which suggests that VA needs to establish standard procedures for identifying telephone requests to prevent unauthorized disclosure of personal information by VA personnel.

Based on our review of VA's plans and documentation for Target and our observations of the pilot operation, we believe that Target has the potential, if properly designed and implemented, for providing a high level of protection of personal information. Because the system has not been implemented, however, we cannot make a complete evaluation of its ability to protect personal information.

VA has implemented a system for controlling terminal-use access to personal information in the pilot program of Target. VA plans to augment and refine this system when Target is implemented.

VA has demonstrated its sensitivity to the need for privacy protection features in its development of the Target System.

VA IS SENSITIVE TO THE NEED TO SAFEGUARD
PERSONAL INFORMATION BUT MUST ASSESS
RISKS TO TARGET MORE THOROUGHLY

insure that adequate controls are established in the system design to avoid costly changes to the system after it becomes operational.

EARLY CONSIDERATION OF THE NEED FOR
PRIVACY PROTECTION FEATURES IN TARGET

In compliance with OMB Circular A-108, dated July 1, 1975, VA submitted to OMB, the Congress, and the Privacy Protection Study Commission a report on new systems in November 1975. This report described the purpose and legal authority for the Target System, VA's evaluation of the effect of the proposed system upon the individual's privacy, and brief descriptions of the protection features proposed for the system to minimize risks to privacy and security.

OMB Circular A-108 requires that the report on new systems be submitted at least 60 days prior to the issuance of a request for proposals for the system's equipment. Because the recipients made no comments on the report, the request for proposals was issued in January 1976. 1/

SAFEGUARDS IN THE PILOT PROGRAM

The requestor cannot gain access to automated record data through the visual display terminals without the appropriate password.

Each terminal user is authorized by regional office management one or more operator commands to the system in line with user duties and the "need to know." Each terminal operator is assigned a unique password which the operator must enter on the terminal together with his/her name for each command given to the system. This minimizes the possibility of anyone using a terminal left active by a previous operator. The password is not shown on the visual display terminals nor is it printed during normal terminal operations, and is seen only on exceptional occasions associated with the security officers' use of terminals.

1/After inquiries by the House Appropriations Committee about the economic justification for four regional computer centers selected for Target, the request for proposals was suspended. On June 15, 1976, the General Services Administration issued an amended request for proposals prescribing three regional centers.

The operator is allowed to execute only those commands known to the system as authorized for his/her use. The password restricts not only the commands available to the user but also the types of records which the user can access. Records pertaining to certain people are designated by VA as "locked" or sensitive. The sensitive records include those of VA employees, very important people, and other veterans who the regional director determines as sensitive because of the nature of the contents of their records or public interest in the veteran concerned.

Those employees who can access sensitive records are determined by the regional office director and are limited to a select few.

The security program in the computer system at Philadelphia monitors and logs attempts to (1) execute unauthorized commands or (2) retrieve data to which a terminal user is not authorized access. The security program issues a daily report containing information on the security violation, the time, the terminal at which the violation occurred, and who made the violation.

All that can be printed on a terminal is the information displayed on the video screen. This is done by pushing a terminal key. This restricts printed data to those authorized and minimizes extraneous printouts requiring controlled disposal.

Terminals in the regional offices can communicate with the regional computer only during regional office working hours. The regional computer center controls activation of the terminals for communication with the automated files.

Each regional office in the pilot program has a security officer whose duties include authorization, control, and distribution of passwords to authorized employees and reviewing the daily violations logs for appropriate follow-up and resolution of violations.

Operator passwords are given by the computer system upon authorization by the security officer and are distributed to each terminal user. The security officer instructs the terminal user on his/her responsibilities for protecting the password and the confidentiality of the data to which the user has access. The user must sign a statement which describes his/her responsibilities. Passwords in the computer system are changed periodically at no fixed schedule.

At the Hines computer facility, where programming is performed for the pilot operation, access by programmers to the production and test files is also controlled by authorized passwords. Access to certain parts of the computer center is controlled by electronically coded cards which designate the areas personnel are authorized to enter. Admission to critical areas, such as the computer room, is gained by electronically coded cards, whose use is logged automatically. The log is reviewed daily by the installation security officer. The mechanized access system is supplemented by security guards.

Access to the Philadelphia center's computer room is also controlled by electronically coded cards.

Additional protection features planned for Target

When Target equipment is installed, VA plans to have locks on the terminals in the regional offices with keys provided to designated supervisory personnel who will lock and unlock the terminals each day at the opening and closing of business.

Authorized terminal users will also be furnished with magnetically coded badges which will identify the user to the security program in the computer and which must be inserted into the terminal before the user can communicate with the system.

In addition, the terminals will be equipped with audible alarms which will sound when certain security violations are committed by the terminal users. The request for proposals for the Target terminal equipment specified that the equipment must include the badge reader, key lock, and audible alarm features.

Training on privacy and security to VA personnel

Since the Privacy Act was enacted on December 31, 1974, VA has provided training to central office and regional office employees through lectures, conferences, operating manuals, regulations, and information circulars explaining their responsibilities under the act.

With regard to Target, regional directors and selected personnel in regional offices have been briefed on regional office employee responsibilities in privacy and security

matters relating to Target. VA plans to use these methods in training terminal operators and supervisors as the system is implemented.

A POTENTIAL WEAKSPOT SHOULD BE
STRENGTHENED IN TARGET

A major objective of Target is to provide prompt service to veterans. This includes providing immediate response to veterans who make inquiries over the telephone regarding the particulars of their claims and benefits. This capability is provided in Target to veterans' services representatives in the VA regional offices through the visual display terminals which can quickly access the automated claims files. Accordingly, veterans' services representatives will be making immediate decisions on releasing personal information.

We noted in our observation of pilot operations in Philadelphia that there are no standard procedures for identifying callers to the telephone unit, where inquiries are resolved in many cases through use of the visual display terminals. The degree to which the requestor's identity is verified is left up to the discretion of the VA veterans' services representatives.

In cases where individuals say they are personally involved in a claim or benefit, the information on visual display can be used for proper identification. However, adequate identification standards to be uniformly and consistently applied by veterans' services representatives, should be developed to minimize the risk of inadvertent information disclosure to someone requesting under false pretenses.

EFFORTS TO DETERMINE THE LIKELIHOOD
AND COST OF EXTERNAL INTRUSION

A basic feature of Target is that information related to CP&E claims and benefits will be electronically transmitted between five computer centers and about 2,500 display terminals and 700 printers located throughout the country. Communications lines, dedicated to only the Target System, will link each regional office with one of three regional computer centers and each regional computer center to the Target central facility and the automated claimant locator system.

In January 1976, VA elicited the assistance of the National Security Agency in identifying Target's

communications threats and the protection that encryption 1/ would provide for these threats.

In August 1976 the National Security Agency advised VA on the types of vulnerabilities a communications-based system such as Target would be exposed to and the protection afforded by encryption and other communications safeguards.

The final decision on whether to use encryption will be made by VA as part of its risk assessment and will be based on an assessment of the degree of risk of intrusion together with the cost of the measures which would protect against such intrusion.

NEED FOR A RISK ASSESSMENT

VA's main thrusts to date to safeguard personal data in the Target System have focused on the use of the visual display terminals in the VA regional offices and the need for encryption. These techniques can be categorized as computer system network controls and represent techniques available in the hardware and software of a computer system or network for controlling the processing of and access to data. However, data integrity and security in automated systems are not necessarily dependent on complex computer system or network controls--this can be substantially achieved by prudent use of physical security measures and information management practices.

VA must now develop a comprehensive risk management program for Target addressing a mix of computer system network controls together with physical security measures for protecting the system's facilities against environmental hazards or deliberate actions as well as information management practices for collecting, validating, processing, controlling, and distributing data.

No system can be completely secure against all the risks of privacy violations; however, the careful selection of a well-balanced set of safeguards, combining both technical and procedural controls, can usually improve the level of protection at a reasonable cost. Before VA can attain this, it must first determine and assess the security risks to the Target System.

1/Encryption is the technique of coding and decoding data moving over communications lines to protect the data from intrusion and monitoring by unauthorized parties.

The goal of a risk assessment is to identify and assign priorities to events which would compromise the integrity and confidentiality of personal data. The seriousness of a risk depends both on the potential impact of the event and its probability of occurrence.

VA intends to do the following in its risk assessment: (1) list all threats to the system, (2) determine the probability of occurrence of each threat, (3) evaluate existing controls for each threat, (4) study the feasibility of additional controls to prevent each threat, and (5) assess the cost effectiveness of the measures to prevent each threat.

A security risk assessment should benefit VA in three ways; it should

- provide a basis for deciding whether additional security safeguards are needed,
- ensure that additional security safeguards will help to counter all serious security risks, and
- save money that might be wasted on safeguards which do not significantly lower the overall risks and exposures.

Need for participation by
Office of Inspector General

As of March 1978, the plan for the conduct of the risk assessment for Target had not been finalized. We were told, however, that the Office of the Inspector General had no plans to participate in the risk assessment. We believe that participation by the Office of Inspector General in the risk assessment is essential because a risk assessment should analyze risks not only to personal data but to other valuable data such as financial data.

It should be noted that the Target System is a benefit payment system from which billions of dollars are disbursed annually. Most of the safeguards for protecting personal data also provide protection to financial data.

The Assistant Inspector General for Audit contends that participation in the risk assessment would bias the independence of the auditors in their review of the system's controls. However, we believe that the internal auditors should be consulted in the development, design, and

testing of automated systems and could advise the risk assessment team of the risks to which a financial system is vulnerable.

Because Target is still in the development stage, participation by the Office of Inspector General in the risk assessment can help ensure that adequate controls are established and adequate audit trails are provided in the system design to avoid costly changes to the system after it becomes operational.

CHAPTER 4

TARGET IMPACT ON THE COLLECTION AND TRANSFER OF PERSONAL INFORMATION

VA does not plan to use Target to collect more information on CP&E recipients than that maintained in its current system. However, its capability for reporting on these individuals could be considerably more sophisticated when the system is fully developed. If this capability is reached, VA may need to tell the public more specifically what information about individuals is being released, and to whom, to keep the public fully informed.

COLLECTION OF INFORMATION IN TARGET

Section 3(e)(1) of the Privacy Act requires that each agency maintain in its records only such information about an individual as is relevant and necessary to accomplish a legitimate purpose of the agency. Section 3(e)(2) of the act further requires that the agency collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about the individual's rights, benefits, and privileges under Federal programs.

One of our concerns in this review was whether VA planned to use Target to collect more information on CP&E recipients than that collected and retained in the current CP&E system as a basis for adjudication and paying claims. According to current VA plans, Target will not expand the type or categories of information maintained in the manual or automated files of the current CP&E system. However, the final design of the Target data base has not been completed. VA collects the bulk of its information on CP&E recipients directly from claimants, their authorized representatives, or from other sources with the permission of the claimant. Other sources of information include the military services which provide information on military service, active duty separation, and medical records related to treatment in service; private doctors and hospitals; and training institutions, which certify attendance and enrollment of the education benefit claimants.

One exception to this rule is the interchange between VA and the Social Security Administration (SSA) whereby VA provides SSA with computer tapes identifying compensation and pension (C&P) recipients who have provided VA with

their social security numbers. SSA in turn verifies the numbers and provide to VA the monthly social security benefit amounts of pension recipients. VA uses this as a basis for computing benefits due to these recipients.

This exchange first occurred in 1973, but subsequent to that time SSA would not provide that information because of its concerns regarding the Privacy Act.

Effective September 30, 1976, the Administrator of Veterans Affairs was authorized by the Veterans and Survivors Pension Adjustment Act of 1976 (Public Law 94-432) to obtain from Federal agencies information for determining eligibility for, or amount of, benefits or verifying other information with respect thereto. This legislation enabled the reopening of the aforementioned exchange between the agencies.

This process was resumed in 1977 and VA plans to receive this information annually to verify incomes claimed by these recipients and adjust their pension benefit amounts accordingly.

TARGET'S REPORTING CAPABILITY

The basic difference between Target and the current CP&E systems is that much of the information on claimants will be more readily accessible in Target. Ready accessibility to information in Target will have two dimensions. First, access to users will be expedited by the visual display of automated records on terminals in the VA regional offices. Second, a principal objective of Target is to provide a flexible reporting system for internal and external users. The technology of Target could enable it to generate considerably more information from the automated records than the current CP&E system. We cannot assess the impact of Target's reporting capability on external release of information because VA is presently designing the Target Central System which should provide this capability.

VA has established policies controlling internal use and external release of personal information from the CP&E records (see p. 8), with no change in these policies contemplated for Target.

In addition VA has established and published in the Federal Register 30 routine uses for information in Target which can be released to external parties without the permission of the individuals on whom the records are

maintained. (See app. I.) These routine uses are the same as those of the current CP&E system.

Three of these routine uses involve transfer of information on computer tapes to outside parties for their use. They are (1) payment data to the Treasury Department for delivery of checks due CP&E beneficiaries, (2) data on the C&P recipients to SSA which are used by SSA to verify eligibility for Supplemental Security Income (SSI) benefits, and (3) data on C&P benefit recipients to the finance activities of the service departments in cases of veterans who have waived all or part of their military retirement pay to receive C&P benefits.

With regard to the SSI interchange, VA has been sending selected data on all C&P recipients but is working with SSA to limit the exchange to only those C&P recipients who are receiving SSI benefits.

Many of the routine uses in Target are broadly stated and thereby allow VA considerable flexibility in applying them to specific release of information.

We noted in our report to Congressman John E. Moss ^{1/} on VA's release of information from its C&P records to SSA for SSI verification that the routine uses cited by VA for releasing this information were so broadly stated that the public might not be fully informed that information maintained by VA was being disclosed to SSA. We recommended that the routine uses be revised to specifically provide for this disclosure. In March 1978, VA informed the Congress that the routine use statements would be so revised.

As Target's reporting system becomes more sophisticated with regard to generating information from the automated records, VA might well need to state more specifically the routine uses of the information to keep individuals fully apprised of what information is being disclosed and to whom.

^{1/}"Privacy Issues and Supplemental Security Income Benefits" (HRD-77-110, Nov. 15, 1977).

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

CONCLUSIONS

VA is sensitive to the need for privacy protection features in its development of the Target System and has used its pilot operation as a tool for developing such safeguards.

We believe that Target has the potential, if properly designed and implemented, for providing a high level of protection of personal information. Because the system has not been implemented, however, we cannot make a complete evaluation of its ability to protect personal information.

We noted one potential trouble spot in our observation of the pilot operation which suggests that VA needs to establish standard operating procedures for identifying telephone requestors of information to prevent unauthorized disclosure of personal information by VA regional offices.

VA's efforts to date to establish appropriate safeguards for Target have been piecemeal and VA needs to more thoroughly assess risks of privacy violations in the total Target system environment to provide assurance that it has selected adequate yet cost-effective safeguards to protect personal information. VA recognizes this need and has plans to perform a risk assessment before Target starts operation.

VA's Office of Inspector General had no plan to participate in the risk assessment. However, we believe that such participation is essential because Target is a payment system from which billions of dollars are disbursed annually and the risk assessment should analyze risks not only to personal data but to financial data as well. Most of the safeguards for protecting personal data also provide protection to other valuable data.

Because Target is still in the development stage, participation by the Office of Inspector General can help assure that adequate controls are established in the system design so that costly changes will be avoided after the system is operational.

VA does not plan to use Target to collect more information on CP&E recipients than that maintained in its current system. However, its capabilities for reporting on

these individuals could be considerably more sophisticated when the system is fully developed. If this capability is reached, VA may need to tell the public more specifically what information about individuals is being released, and to whom, to keep the public fully informed.

RECOMMENDATIONS TO THE ADMINISTRATOR
OF VETERANS AFFAIRS

We recommend that the Administrator direct the Office of Inspector General to participate in the risk assessment of the Target System. We further recommend that the Administrator direct the Department of Veterans Benefits to establish standard procedures before the start of Target for identifying telephone requestors to prevent unauthorized disclosure of personal information by VA personnel.

ROUTINE USES OF
TARGET SYSTEM RECORDS
PUBLISHED IN THE FEDERAL REGISTER
SEPTEMBER 27, 1977

1. Transfer of payment information to the Treasury Department to ensure delivery of benefit checks to VA beneficiaries.
2. Transfer of information to collection agencies in order to conduct a credit check to determine the likelihood of success in a collection action against individuals who owe debts to the VA.
3. Transfer of necessary collection information to the General Accounting Office for use in procedures incident to obtaining a judgment against the individual.
4. Forwarding of computer generated VA forms to VA-approved educational institutions in order to certify an individual's re-enrollment and allow payment.
5. Transfer of information regarding the induction, re-entrance and dismissal of a disabled veteran from a vocational rehabilitation program to inform the training establishment of the actions taken.
6. Written and oral disclosures to a VA-approved vocational rehabilitation training establishment regarding the extent and nature of a claimant's disabilities with respect to any limitations to be imposed on the vocational program to ensure that the trainee receives the maximum benefit from training. A vast amount of discretion with respect to each disclosure is practiced.
7. Transfer to schools and other training establishments of VA education forms for completion by the school and subsequent submission to the VA for processing of education and vocational rehabilitation training claims.

8. The transfer of payment information to officials of schools and training establishments having VA beneficiaries when it can be determined that such request is part of a legitimate attempt to assist the veteran or other eligible person to ascertain that correct amounts are paid. However, such information will not be provided as a routine use to school officials when the request is clearly an attempt to seek assistance in collection attempts against the veteran or eligible person.
9. Transfer of VA education letters and form letters to schools and other training establishments which may, by necessity, contain identifying data about a veteran or eligible person in order to obtain further information from the school necessary to discharge VA responsibilities toward the veteran or eligible person.
10. Transfer of identifying information, such as name, file number, and address to a school training establishment official in order to obtain information necessary to pay the veteran or eligible person correct amounts in an expedited manner. (An example of the above is a telephone call to an On-The-Job-Training establishment to find out the number of hours worked.)
11. Transfer of necessary information concerning veterans and other eligible persons to State and local agencies and prospective employers for employment and/or training.
12. A record containing medical history, diagnoses, findings, or treatment may be released from this system of records in response to a request from the superintendent of a State hospital for psychotic patients, a commissioner or head of a State department of mental hygiene, or head of a State, County, or city health department, or any fee basis physician or institution in connection with authorized treatment as a VA beneficiary, provided that the name of the individual to whom the record pertains is given and that the information will be treated as confidential, as is customary in civilian professional medical practice.

13. A record from this system of records may be disclosed to a State unemployment compensation agency, in response to its request, to the extent required to determine eligibility for their benefit.
14. A record from this system of records may be disclosed to the following agencies relative to military, naval, or air service and as to both current and historical benefit payments made by the VA; Departments of the Army, Navy, and Air Force; Marine Corps; Department of Transportation (Coast Guard); Department of Health, Education, and Welfare, PHS (Public Health Service), Commissioned Corps; Department of Commerce, NOAA (National Oceanic and Atmospheric Administration), Commissioned Officer Corps.
15. A record from this system of records may be disclosed to a third party to the extent necessary in the development of a potential beneficiary's claim for VA benefits (i.e., individual identifiers and other similar identifying information).
16. A record containing the name(s) and address(es) of present or former members of the armed services and/or their dependents may be released from this system of records under certain circumstances: (1) to any nonprofit organization if the release is directly connected with the conduct of programs and the utilization of benefits under Title 38, and (2) to any criminal or civil law enforcement governmental agency or instrumentality charged under applicable law with the protection of the public health or safety if a qualified representative of such organization, agency, or instrumentality has made a written request that such name(s) or address(es) be provided for a purpose authorized by law; provided, further, that the record(s) will not be used for any purpose other than that stated in the request and that the organization agency or instrumentality is aware of the penalty provision of 38 U.S.C. 3301(f).
17. The amount of pension, compensation, dependency and indemnity compensation, educational assistance allowance, retirement pay and subsistence allowance, of any beneficiary, may be released from this system of records to any person who applies for such information.

18. Disclosure of VA records as deemed necessary and proper to accredited service-organizations, agents and attorneys recognized under a power of attorney or declaration of representation to assist in the preparation, presentation and prosecution of claims.
19. A record from this system of records may be disclosed to a fiduciary (including those acting in a fiduciary capacity) recognized or appointed by the VA to the extent necessary to fulfill the fiduciary's function.
20. Relevant information from this system of records may be disclosed; as a routine use. in the course of presenting evidence to a Court, magistrate, or administrative tribunal, in matters of guardianship, inquests, and commitments; to private attorneys representing veterans rated incompetent in conjunction with issuance of Certificates of Incompetency; and to probation and parole officers in connection with Court required duties.
21. Transfer of statistical and other data to Federal, State and local government agencies and national health organizations to assist in the development of programs that will be beneficial to claimants, to protect their rights under law and to assure that they are receiving all benefits to which they are entitled.
22. In the event that a system of records maintained by this agency to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

23. A record from this system of records may be disclosed as a "routine use" to a Federal, State or local agency maintaining civil, criminal or other relevant information, such as current licenses, if necessary to obtain information relevant to an agency decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant or other benefits.
24. A record from this system of records may be disclosed to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.
25. Relevant information from this system of records, including the nature and amount of a financial obligation, may be disclosed as a routine use, in order to assist the Veterans Administration in the collection of unpaid financial obligations owed the VA, to a debtor's employing agency or commanding officer so that the debtor-employee may be counseled by his or her Federal employer or commanding officer. This purpose is consistent with 5 U.S.C. 5514, 4 CFR 102.5, and section 206 of Executive Order 11222 of May 8, 1965 (30 F. R. 6469).
26. Relevant information from this system of records, including available identifying data regarding the debtor, such as name of debtor, last known address of debtor, name of debtor's spouse, social security account number of debtor, VA insurance number, VA loan number, VA claim number, place of birth and date of birth of debtor, name and address of debtor's employer or firm and dates of employment, may be disclosed to other Federal agencies, State probate courts, State drivers license bureaus, and State automobile title and license bureaus as a routine use in order to obtain current address, locator and credit report

assistance in the collection of unpaid financial obligations owed the U.S. This purpose is consistent with the Federal Claims Collection Act of 1966 (P. L. 89-508, 31 U.S.C. 951-953) and 4 CFR Parts 101-105.

27. Disclosure may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.
28. Release of information to a guardian ad litem in relation to his or her representation of a claimant in any legal proceeding.
29. To the Department of Justice and United States Attorneys in defense or prosecution of litigation involving the United States.
30. Disclosure may be made to NARS (National Archives and Records Service) GSA (General Services Administration) in records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

PRINCIPAL VA OFFICIALS RESPONSIBLEFOR ADMINISTERING ACTIVITIESDISCUSSED IN THIS REPORT

	<u>Tenure of office</u>	
	<u>From</u>	<u>To</u>
ADMINISTRATOR OF VETERANS AFFAIRS:		
J. M. Cleland	Mar. 1977	Present
R. L. Roudebush	Oct. 1974	Feb. 1977
R. L. Roudebush (acting)	Sept. 1974	Oct. 1974
D. E. Johnson	June 1969	Sept. 1974
DEPUTY ADMINISTRATOR OF VETERANS AFFAIRS:		
R. H. Wilson	Mar. 1977	Present
Vacant	Jan. 1977	Mar. 1977
O. W. Vaughn	Nov. 1974	Jan. 1977
Vacant	Oct. 1974	Nov. 1974
R. L. Roudebush	Jan. 1974	Oct. 1974
F. B. Rhodes	May 1969	Jan. 1974
CHIEF BENEFITS DIRECTOR:		
D. Starbuck	May 1977	Present
A. J. Bochicchio (acting)	Mar. 1977	May 1977
R. H. Wilson	Jan. 1975	Mar. 1977
J. J. Mulone (acting)	Nov. 1974	Jan. 1975
O. W. Vaughn	Mar. 1973	Nov. 1974
O. B. Owen	Feb. 1970	Mar. 1973
CHIEF DATA MANAGEMENT DIRECTOR:		
W. R. Martin	Oct. 1975	Present
W. R. Martin (acting)	Aug. 1975	Oct. 1975
R. T. Brown	Aug. 1974	July 1975
P. J. Budd	July 1963	July 1974

(40041)