



17343
114604

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

GENERAL GOVERNMENT
DIVISION

B-201698

MARCH 17, 1981

Mr. H. Stuart Knight
Director, U.S. Secret Service
Department of the Treasury



114604

Dear Mr. Knight:

Subject: The [Secret Service Has More Computer
Capacity Than It Needs] (GGD-81-43)

We have reviewed the use of computers by the Secret Service to evaluate how effectively these resources are managed and how well they contribute towards the accomplishment of the Service's mission. We made our review at Service Headquarters in Washington, D.C., by analyzing available records, interviewing key personnel and senior management in the data processing and user groups, and conducting limited tests of the Service's computerized information systems.

The Service relies heavily on data processing to carry out its protective and law enforcement functions. The capability to store huge volumes of information and retrieve it rapidly is a tremendous asset to the Service. We found, however, that the Service has not adequately defined its data processing requirements and as a result has more computer capacity than necessary. Specifically, the Secret Service has two large high performance computers when one would be sufficient.

Service officials we spoke with cited several reasons why two computers are required. However, we could not find any evidence that the Service had determined the necessity of dual computers before acquiring them or had considered and justified the additional cost of the potential benefits for two computers. The rationale used by the Service to explain why it has two computers is based on requirements that are not being met and, in any event, could be satisfied with a single computer. The expected total cost of both computers over their 6-year life is \$3.5 million. In view of the significant dollar savings which could be realized, the Service should move as quickly as possible to reassess its computer equipment needs.

(260010)

015977

AUTOMATION AT THE SECRET SERVICE

The Secret Service began developing computerized information systems in the mid-1960s. At first, the computer was used to store intelligence files on persons or groups considered to be a threat to the President or other individuals the Service is responsible for protecting. Gradually, the computer was put to other uses, such as assisting in agent assignments and enhancing the Service's enforcement of counterfeiting laws. Today, the Service has three major computerized information systems: Protective, Law Enforcement, and Administrative. Each has various data bases and subsystems that store, process, analyze, and retrieve information for the Service.

For the last 7 years the Secret Service has used two computers to support its three information systems. The Service operated with a single computer until 1973 when, faced with limited capacity, it acquired a larger, more powerful computer that could access, process, and retrieve data instantaneously. After the new computer was installed, the Service kept the older computer which was fully paid for and used both computers for supporting the Service's data processing needs. These computers were replaced in 1976 by two larger identical computers which, in turn, were themselves recently replaced. The two new computers, which have identical central processing units and the same amount of memory, differ only in the number of peripheral devices configured with each. They were acquired for approximately \$3.5 million under a lease/ownership arrangement under which the Service will own the computers after 6 years. The first computer began operating in December 1979 and the second in June 1980.

DOES THE SERVICE NEED TWO COMPUTERS?

The Service could not provide us any material, such as feasibility studies or planning documents, to explain why it requires duplicate computers. Consequently, it does not appear that the Service ever adequately determined the necessity of having two computers, as opposed to one, or that the Service ever considered and justified the additional expense of two computers before acquiring them. Service management told us that they believe two computers are necessary in order to assure rapid response time, maintain adequate security of data, and provide the Service with backup capability should one of the computers malfunction. However, a requirements study was never made by the Service to determine that two computers were needed. Moreover, our tests show that the Service is not realizing any advantages or improvements in accomplishing its mission because it has two computers rather than one.

Data processing requirements
have not been defined

The Secret Service acquired duplicate computers and subsequently replaced them without having determined what its data processing needs were and how they could be met. The decision to use two computers was apparently based on a 1974 consultants' study which did not demonstrate that two computers were necessary but rather only pointed out that two might offer certain advantages over one at only a slightly higher cost. Although the Service had the opportunity to reassess its equipment requirements in 1978 when it replaced its computers, it did not do so. Consequently, the Service continues to use two computers without having ascertained if they are necessary or beneficial.

Soon after the Service had acquired a second computer in 1973 and was continuing to use its older, smaller computer, it hired a consulting firm to determine its data processing requirements and explore the options available to best satisfy them. The consultants' study, issued in 1974, reported that even with its two existing computers, the Service lacked the capacity to accommodate the projected workload that would come with additional computerized information systems that were being planned.

The report noted that, although one large computer could satisfy all of the Service's present and planned requirements, two medium-to-large computers had certain advantages, such as backup capability in the event that one computer failed, enhanced data protection, and increased ability to meet response time requirements. The consultants concluded that the potential advantages of two computers were sufficient to justify the higher cost, which they estimated to be 15 percent, and recommended that the Service consider replacing the then-current equipment with two computers and dividing the processing load between them.

We could not verify the cost estimates of the 1974 study or the required capacity that was forecast because the data was not available. We noted, however, that the study did not address the questions of why, how badly, or for what data, the Service needed quick access, protection, and backup capability. Also, we could not locate any evidence that the Service itself had ever analyzed its needs in these areas. Without having determined exactly what these requirements were, the Service had no basis for concluding that it needed two computers instead of one.

According to officials we spoke with, the increased workload expected with the 1976 presidential election did not leave the Service enough time to competitively acquire the additional capacity recommended by the study. The Service therefore requested authority from the General Services Administration to acquire, on a sole source basis, two identical computers. This authority was granted but with the stipulation that these computers be competitively replaced within 3 years. Consequently, the most recent procurement in 1979 was made because the computers had to be replaced competitively. Neither of the procurements was adequately justified to demonstrate that the Service required two computers. This requirement was apparently based on the 1974 consultants' study which, as pointed out above, also failed to demonstrate the necessity of two computers.

At some point between the 1974 study and the request to noncompetitively acquire identical computers, the determination was made that the protective system would be operated on one computer while the administrative and law enforcement systems would be supported by the other. We were unable to determine who had made this decision or why. Service officials explained to us that this procedure assured the protective system a rapid response rate, rigid security, and backup capability. However, the protective system's requirements for these three attributes have never been defined so that the Service does not have a basis for determining whether the system requires its own computer. It should also be noted that the 1974 consultants' study, upon which the acquisition of two computers was apparently based, did not conclude that the protective system would require a separate computer. In fact, the report pointed out that the system could be run, along with other systems, on a single computer and still allow for quick access and data security. The report also did not state conclusively that backup capability was only possible with two computers.

How rapid a response is necessary?

The Secret Service has not determined how quickly information needs to be retrieved from the protective system and under what circumstances. Consequently, it has no way of determining if two computers are necessary to provide adequate response time. We reviewed the ways in which the protective system is used and found that there are some instances when it is critical that information be relayed to agents in the field as rapidly as possible. However, we do not believe that the system's total response time in these situations would suffer if the Service had

only one computer. Moreover, the Service could explore opportunities to minimize or even eliminate any delays, should they occur, by ensuring that the system is programmed as efficiently as possible.

Any possible delay in the response time of the protective system that might be caused by processing all of the Service's workload on one computer would not be more than a few seconds. In determining an acceptable response rate, the Service should consider how the system is used and under what circumstances seconds would be crucial. The protective system can be used in two ways: an operator can query the computer via a terminal and have the information displayed almost immediately on the terminal's screen (the online mode), or a list of names can be submitted to a computer operator and the desired information printed out some time later (the batch mode). The batch mode is normally used by agents responsible for the advance work related to a protectee's appearance at a public affair. Names are sent to Washington in computer readable form via a teletype machine, processed by the computer, and the results returned via the same device. Turnaround time ranges from a few hours to a day.

Most of the online inquiries to the system are done by intelligence research specialists for updating background information, analyzing trends, or other investigative work. The only way that agents in the field have online access to the protective system is through the duty desk at Service headquarters. This control center is manned 24 hours a day by agents who respond to telephone requests for name searches by using the five terminals located there. These requests come from

- agents at an organized event who have detained someone they consider a possible threat to the protectee or who need to verify someone's identity,
- agents responding to or investigating a threatening telephone call or letter,
- agents who are approached by a suspect at a field office or other location, and
- agents required to use the online mode because a change in a protectee's travel plans did not allow time for name checks to be submitted in batch mode over the teletype.

We do not believe that all of the online users of the protective system require instant access to the system. In our opinion, immediate access to the protective system is most critical in the case of agents at the duty desk responding to requests for name searches from the field. The Service has similar views since the terminals at the duty desk are given priority by the computer over all others. However, only in some situations would seconds be important to field agents; for example, when an individual in the vicinity of a protectee is being questioned. In our opinion, cases such as this are relatively few compared to the total number of name searches that are performed.

According to the very limited Service records available for 1980, the daily average of name searches of the protective system done by batch processing is 697. The daily average of name searches done online is 910, of which 235 are done at the duty desk. Because there are no records kept of why the duty desk agents use the protective system, there is no way of determining how many of the duty desk name searches were done in situations where seconds were crucial. Many, for example, could have been done for advance work or other routine requests for information from the field where seconds are not crucial. In any event, we do not believe that the time required to relay data from the protective system to agents in the field would be discernably increased if the Service had only one computer.

The only part of the response time that is affected by the computer and its workload is the time interval between the terminal operator pressing the last key and the first letter of the reply appearing. The bulk of the total response time for the protective system rests with the capability of the terminal operator and whatever time is required for field agents to reach the duty desk by telephone. Although we cannot be precise unless appropriate technical tests are conducted, we do not believe that processing all three of the Service's systems on a single computer would noticeably increase the total response time of the protective system for agents in the field.

It is entirely possible that the time required by the duty desk terminals to access the protective system would not increase at all should the Service process all three of its systems on a single computer. Without collecting appropriate data and adequate testing it is impossible to be certain. However, because of the speed with which modern computers function, and the fact that the computer already interrupts any other work to respond to inquiries from the duty desk terminals, there is no reason to believe that any delay, should one occur, would be longer than a few seconds. If

this is unacceptable to the Service, it could review the efficiency of the protective system as well as its total data processing operation to ensure that response time is not affected by inefficiencies or bottlenecks and reduce, or even eliminate, this delay.

Data security can be maintained
with a single computer

The Secret Service does not need two computers to protect the confidentiality of information contained in the protective system. Adequate safeguards can be implemented in the system to prevent unauthorized access.

Service officials we spoke with contend that one method for providing security over the protective files is for each computer to have its terminals wired directly to it so that one computer's terminals cannot access information from the other computer. Running the protective system on a separate computer therefore limits the number of terminals that can retrieve data from the system to those directly wired to the computer running the system. However, wiring selected terminals directly to a computer is only one method of protecting the information stored on that computer.

Another, more commonly used method is to program internal controls into a computerized system itself. Safeguards could be installed in the protective system that would allow access only from certain terminals. Passwords could be used to allow access to only authorized users. Access to certain files could be restricted to only a few individuals or made dependent upon the time of day or both, and a record kept of who accessed what file. In short, there are a number of programming controls that could be implemented to make the protective system reasonably secure.

Some of these controls are already being used by the Service. During the recent presidential campaign, a personnel management system for assigning agents to candidates was run on the same computer as the protective system. Access to the personnel system was also through online terminals, but we were informed that appropriate internal controls had been installed to prevent these terminals from being used to obtain information from the protective system.

In any event, the most stringent security measures within the computer room are pointless as long as unauthorized disclosure is possible elsewhere. In our opinion, the use of telephones to relay information from the protective files to agents

in the field is significantly riskier than the risks associated with the use of computer terminals, since lines can be tapped or otherwise penetrated. Furthermore, agents at the duty desk will normally furnish information simply on the basis of voice recognition. Although an identifying code might be asked for if there are any doubts, we believe the risks associated with these procedures for furnishing information negate any potential advantages of using dedicated terminals.

Two computers are not providing the Service with backup capability

The advantages of having a second computer available for emergency processing of the protective system would appear to be obvious. However, the proximity of the computers to one another would cause both to go out of service in the event of a major emergency, such as a fire, explosion, or loss of electricity. Moreover, the protective system has only rarely been switched over to the other computer because of its computer malfunctioning, and the Service already has a means of keeping the protective files available for field agents so that duplicate computers are unnecessary.

The necessity of keeping the protective system functioning is a valid one. Agents in the field need to have constant access to information that is vital in assessing threatening situations and determining who they might be dealing with. Service officials we spoke with felt that this requirement was being satisfied by having two computers. In the event that the computer supporting the protective system broke down, the system could be transferred to the other computer within 15 minutes and disruption would be minimal. It does not appear, however, that this procedure is followed very often. More importantly, the same information could be provided to field agents from manual records, should the computer break down, with a minimal increase in the time required.

We reviewed the daily operating logs kept by computer room personnel and found that the computer supporting the protective system was out of operation for 10 minutes or longer a total of 65 times during the 1-year period ending December 1, 1979. On average, these disruptions occurred once every 5-1/2 days with an average downtime of 3 hours and 46 minutes. According to the operating logs, in only one instance was the protective system switched over to the other computer. Because these logs might be incomplete, we asked computer room

employees how often the system was transferred due to computer breakdown. They estimated that this had occurred only 5 to 10 times during the 1-year period. Switching the system from one computer to another was not even possible from December 1979 until October 1980--the height of the presidential campaign--while the Service was converting from the old computers to the new. During this period, the Service had no backup for the protective system except for the manual files.

The duty desk keeps a computer printout of all individuals whose names are in the protective system. With this alphabetical listing, which is updated daily, an agent at the desk can determine an individual's status and whether an investigative profile exists. If so, the entire manual case file can be retrieved from a room immediately next to the duty desk. We tested how much additional time this would require and found that, on average, it took 22.5 seconds for an agent to type a name onto a terminal and determine if the person was listed in the system. For an agent to determine this from the printout required an average of 49 seconds. If a profile existed, the terminal operator could call it up in 16 seconds from the computer, whereas 1 minute and 5 seconds was needed to retrieve the entire file from the next room.

Because the protective system has different uses, the Service should consider its contingency requirements accordingly. In terms of how agents at the duty desk use the system, we believe that the available manual files already provide a reasonable alternative means of providing field agents information they might urgently need should the computer break down for short periods of time. Consequently, we question the necessity of having two computers so that one could be used as backup when the other is inoperative due to more or less normal disruptions.

The possibility of the computer being out of service for more than several days, thus preventing any use of the protective system, is remote and would most likely be caused by some physical catastrophe such as a fire or explosion. Because both of the Service's computers are located in the same room, both would probably be put out of commission by such a disaster. Therefore, having a second computer for backup purposes during an extended period of downtime is also questionable. A commonly used means of dealing with extended downtime is to make prior arrangements with another facility with compatible equipment to share computer resources in the event of an emergency. In fact, the Service already has an agreement with another Government

agency to use its facility to run the protective system should the Service's computer be inoperable for more than 2 days. This arrangement casts further doubt on the advisability of the Service keeping two computers so that one is always available should the other suffer extensive damage.

Having an extra computer onsite for backup purposes can assure continued operations in only a limited set of circumstances. As pointed out above, we believe that the benefits which might be derived are limited and doubt if they justify the extra cost. Rather than adopting such extreme measures, the Service could better serve its mission requirements by ensuring that more basic emergency plans are in place. For example, the Service does not have an alternate source of power available for either computer. Consequently, both computers would stop functioning should the facility suffer an electrical outage. Additionally, the contingency plan has never been tested so that the Service cannot be certain the protective system will run on the alternate computer. An agreement with an agency with a like computer does not guarantee compatibility. Potential differences in operating systems and computer configurations could render the arrangement useless.

THE SECRET SERVICE HAS EXCESS COMPUTER CAPACITY

The Secret Service does not need two computers for its data processing workload. On the basis of our review of the limited computer utilization data available, we believe that one of the Service's two computers has more than enough processing power and capacity to handle the current workload as well as increases planned for the future. While the Service believes that a single computer would lack sufficient memory, it cannot be certain without an adequate analysis of the machine's requirements. In any event, the memory capacity of a single computer could be substantially increased. Exactly how much excess capacity the Service has cannot be determined until performance monitoring systems are used to measure computer resource utilization.

There is no question that one of the Service's computers is powerful enough to accommodate the data processing workload. We were informed that, prior to their replacement, neither of the Service's two computers had any performance limitations regarding the machines' central processing units. The computers that were recently acquired have processing units approximately twice as powerful. The Service's computer workload, however,

has not been increased. Consequently, if two computers had sufficient processing power for the Service's needs, one computer with twice the processing power should meet the same requirements.

Service officials told us their concern was that a single computer would not have enough memory capacity to do all the work. In the absence of any analysis by the Service demonstrating that memory would be limited, we asked the Service to measure the amount of memory available on each computer for the busiest shift for 1 typical day. Their results showed that 33 percent of one computer's memory and 75 percent of the other's were never used during the shift. This could be interpreted to mean that had one computer been operating, 92 percent of its memory would have been used at least at one point during the shift. Without more detailed analysis, however, it is not possible to be certain how much memory is required.

Several factors make the Service's results inconclusive. For example, when the measurements were taken, several programs with large memory requirements were being run simultaneously on both computers for testing purposes. Ordinarily, these programs would be run on only one computer. Additionally, a single measurement is not sufficient testing on which to base any conclusions. Most importantly, however, the Service has not considered several factors which could reduce the amount of memory that its information system might require. For example, it is possible that memory requirements could be reduced through more efficient programming. Also, the Service could consider the possibility of processing certain work only during the second and third shifts, thereby making more memory available during the prime shift. To assist in evaluating these types of changes, the Service should acquire the necessary performance monitoring systems so that their impact can be measured. In addition, the information provided by the performance monitoring systems can be used to begin a concerted effort to assure that computer resources are being used as efficiently as possible.

On the basis of the data currently available, we believe that one of the Service's computers, which has twice the memory capacity that both of the old computers had, has sufficient memory to handle the workload. Should the Service, however, ascertain that this is not enough, the memory capacity of one of its computers could be as much as doubled by the addition of increments of memory. This would give the Service 4 times as much memory as was available on both of the computers that were replaced in 1979.

According to the figures given us by the Service, about \$800,000 of the total projected cost of \$3.5 million for both computers has already been spent. Most of this expense was for conversion and installation costs. We cannot specify how much of the remaining costs could be avoided until the Service determines such things as its exact equipment requirements; reductions in utilities, space, maintenance and personnel; and the modifications the remaining computer might require. The potential savings could approach, equal, or even exceed half of the projected remaining costs.

CONCLUSIONS

The Secret Service has computer resources in excess of its requirements. Because the Service did not define its data processing needs beforehand, it has acquired two separate and identical computers when one would have been sufficient for the workload. The rationale used to explain the necessity for two computers is not supported by any analysis of what the Service's response time, security, and backup requirements are and how these needs can only be met by two computers. Consequently, the Service has no basis for determining that it needs two computers or if it is realizing any advantages from having two.

We believe that one of the Service's two computers has enough processing power and memory capacity to handle the current demands as well as any planned increases. However, before the specific excess equipment can be identified, the Service will need to measure precisely what its computer needs are and assure itself that these needs are being met in the most efficient and effective manner. The Service has just completed the first year of a 6-year leasing arrangement expected to have a total cost of \$3.5 million. Perhaps as much as half of the remaining costs could be avoided over the next 5 years if the Service expedites a thorough analysis of its computer requirements and returns unnecessary equipment to the manufacturer.

RECOMMENDATIONS

We recommend that the Secret Service take immediate steps to define its data processing requirements and ensure that its computer resources are commensurate with its needs. Specifically, the Service should:


- Perform a cost-benefit analysis of its data processing requirements and determine the equipment necessary to support these needs. At a minimum, this analysis should establish criteria to define and quantify the computer response time, security, and backup requirements for the Service to carry out its mission; explain the justification of these requirements; and demonstrate how the equipment necessary to meet these needs was decided on.
- Obtain and install the necessary performance monitoring tools to measure computer utilization and use this information as a basis to ensure that data processing resources are being used as efficiently as possible. This will also assure that only necessary resources are acquired.

- - - - -

We have discussed our findings with the Assistant Directors for Protective Research and Administration and other Service officials during the course of our review and after its completion. These officials generally agreed with the problems we identified and our recommendations, particularly with the necessity for the Service to measure the computers' utilization and capacity.

Copies of this report are being sent to the Secretary of the Treasury, the Director of the Office of Management and Budget, and interested congressional committees. We would also appreciate being advised of any actions you plan to take on the matters discussed in this report.

Sincerely yours,



William J. Anderson
Director