NBSIR 77-1262

Computer Site Security Monitor and Response System

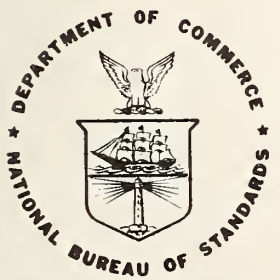
R. T. Moore
R. J. Carpenter
A. L. Koenig

Computer Systems Engineering Division
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

Sponsored by

Defense Nuclear Agency
Washington, D.C. 20305

June 1, 1977



U. S. DEPARTMENT OF COMMERCE
NATIONAL BUREAU OF STANDARDS

NBSIR 77-1262

COMPUTERIZED SITE SECURITY MONITOR AND RESPONSE SYSTEM

R. T. Moore
R. J. Carpenter
A. L. Koenig

Computer Systems Engineering Division
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

Sponsored by

Defense Nuclear Agency
Washington, D.C. 20305

June 1, 1977

U.S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, *Secretary*

Dr. Sidney Harman, *Under Secretary*

Jordan J. Baruch, *Assistant Secretary for Science and Technology*

NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Acting Director*

COMPUTERIZED SITE SECURITY
MONITOR AND RESPONSE SYSTEM

SECTION I. Summary Report of Phase I Findings

Section II. System Description

Section III. Proposed Phase II Work Plan

COMPUTERIZED SITE SECURITY
MONITOR AND RESPONSE SYSTEM

ABSTRACT

The Computerized Site Security Monitor and Response System (CSSMRS) was conceived as an integrated, state-of-the-art, computer-based system to enhance and improve the overall physical security of storage sites for special weapons or materials.

This report is divided into three sections. Section I contains an overview summary of the findings or study results for each of the eight specific Phase I tasks. These are set forth in varying degrees of detail as appropriate to both the nature of the task and the results.

Section II is a description of the CSSMRS in its current (and incomplete) state of evolution. Here many of the attributes, capabilities, and features developed during the course of Phase I work are set forth. Some of the alternatives are identified as are areas where additional work will be necessary to reach clearly identifiable and attainable objectives necessary to complete the system definition.

In Section III, a proposed Phase II work plan is presented.

INTRODUCTION

The Computerized Site Security Monitor and Response System (CSSMRS) was conceived as an integrated, state-of-the-art, computer-based system to enhance and improve the overall physical security of storage sites for nuclear weapons or materials. This would result from the interconnection of all site security systems including intrusion detection equipment, duress alarms, guard radio and telephone systems, guard activity sensors, meteorological sensors and deterrent systems to a computer to provide timely, accurate and unambiguous information about the site security status or the progress of an attack or intrusion attempt and the programmed response that would best counter it. Changes in site security status and resulting response actions would be automatically reported up-channel to higher command and to backup and reserve forces which would be automatically called out in the event of certain identifiable threat situations, and, in particular, those in which the continued survival of local guard forces might be in doubt. Under these circumstances, certain deterrents would also be activated.

Because of the broad scope of the CSSMRS concepts, effort on them was programmed in three phases. Phase I is concerned with fact-finding, data collection and analysis, feasibility research and with the identification of specific areas where supporting research and development efforts might be required. Phase II covers system definition, design and specification, and Phase III the implementation, test and evaluation of one or more prototypes. Under Phase I, nine specific tasks were identified. Eight of these involved data collection, analysis, consultation or research and development, and this, the ninth, covered the summary documentation of these findings, together with a proposed Phase II work plan.

In addition to this summary report, topical reports covering each of the individual tasks have been submitted to the designated DNA Subtask Manager.

This report is divided into three sections. Section I contains an overview summary of the findings or study results for each of the eight specific Phase I tasks. These are set forth in varying degrees of detail as appropriate to both the nature of the task and the results.

Section II is a description of the CSSMRS in its current (and incomplete) state of evolution. Here many of the attributes, capabilities, and features developed during the course of Phase I work are set forth. Some of the alternatives are identified as are areas where additional work will be necessary to reach clearly identifiable and attainable objectives necessary to complete the system definition.

In Section III, a proposed Phase II work plan is presented.

SIMPLIFIED BLOCK DIAGRAM OF CSSMRS

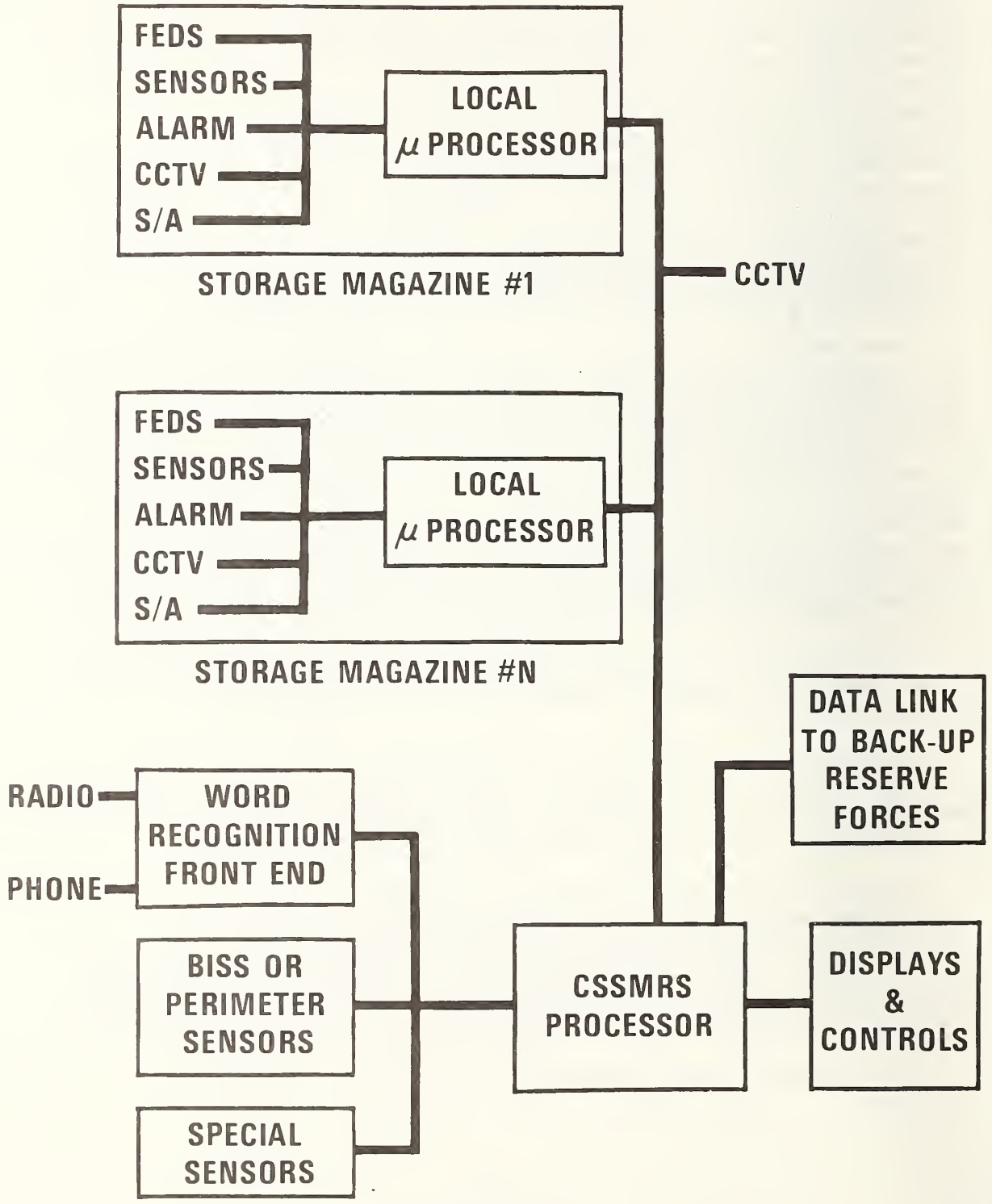


FIGURE 1

Section I

Summary of Phase I Findings

Task 1. Collection and analysis of information on the detailed characteristics of the Base and Installation Security System (BISS), the Facility Intrusion Detection System (FIDS), the Forced Entry Deterrent System (FEDS), the Joint Service Interior Intrusion Detections System (JSIIDS) commercial alarm systems, Closed Circuit Television (CCTV) and security communications equipment. This includes a critical review of potential CSSMRS interfaces in each system component, including their physical and electrical features.

Findings: Data have been collected on BISS, JSIIDS, FIDS, and FEDS equipments, both presently in existence and planned, as well as on commercial intrusion alarm equipments, closed circuit television, and security communications equipment. In general, there do not appear to be any extraordinary problems involved in interfacing appropriate components of any of these systems to the CSSMRS. The term "components" has been used advisedly in this connection. In the course of their development, there has been a tendency for each security system to be endowed with an independent control unit, annunciator panel, and data communications capability. In most instances, these system components accomplish functions which will be handled in a more efficient, effective, and integrated manner in the CSSMRS, and, in these cases, interfacing would best occur at the level of sensor or sensor signal processor.

The evolving concept of the CSSMRS appears in simplified block diagram form in figure 1 as a distributed array of microprocessors communicating with a central CSSMRS processor which, in turn, maintains communications up-channel with higher headquarters as well as with special sensors, processors, displays, and controls. Each of the local microprocessors normally functions as a slave to the central CSSMRS processor, and, in this capacity "handles" a localized group of sensors and intrusion deterrents in accordance with authenticated instructions received from the master or by exercising pre-programmed initiatives. Response functions performed by the local microprocessor include access/normal and safe/arm establishment, sensor-testing and status-reporting, driving closed-circuit television camera controls and actuating forced entry deterrents (FEDS). Functions performed under pre-programmed initiatives include the generation of an interrupt signal and an appropriate message to the CSSMRS processor if an alarm occurs, monitoring CSSMRS status and reverting to an autonomous mode of operation in the event of communication or CSSMRS central processor failure. In the autonomous mode,

any current "access" status will be revoked and FEDS will be activated automatically in multiple alarm conditions that persist beyond an appropriate time limit.

The foregoing brief and incomplete description of the CSSMRS heirarchical control concepts is intended only to provide general insight regarding the appropriate level of interfacing to existing or planned security system sensors and components.

TASK 2. Examine the existing data regarding correlation between nuisance alarms and certain readily identifiable meteorological events, such as lightning and wind which are known to influence some types of intrusion detection sensors. Suitably high levels of correlation might form a basis for recognition and rejection of some portion of the naturally caused nuisance alarms through the time-phased comparison of the signals from meteorological or other environmental background sensors and intrusion detections sensors. Determine the desirability or need for further research in this area.

Findings: In connection with the BISS program, studies have been conducted to determine the performance of various types of perimeter sensors and the effect of meteorological phenomena or other sources of background energy on detection probability and nuisance alarm rates.

Allen, et al (1) reported on the performance of several types of perimeter sensors with respect to 4,295 intrusion attempts and 2,363.8 hours of false alarm monitoring during which environmental and site background data were collected. The authors note that the false alarm susceptibility of the sensors varies with the environment which the transducers see and suggest that the moisture content of the soil, the seismic, electromagnetic, and acoustic background noise at the site are factors whose influence on the sensor might be controlled by the signal processing electronics attached to the transducer. They state the opinion that false alarm data is usually misleading unless coupled with information on the specific environment encountered and recommend that special emphasis should be given in any future testing to false alarm rejection.

---

(1) Buried Line Sensor Evaluation for BISS Part II - 1975 - Evaluation Results, Proceedings 1975 Carnahan Conference on Crime Countermeasures, University of Kentucky BU107, May, 1975.

Underdown, et al (2) reports on fence penetration sensors and wind-induced nuisance alarms. The tests indicated the advantage of using processing logic for both cable-type and switch-type sensors; this logic had the effect of increasing the wind speed that could be tolerated without excessive nuisance alarms. This advantage may be offset by a decreased ability to detect the relatively small vibrations imparted to the fence by skillful or ladder-assisted climbers. The authors conclude that improvement in the ability of fence sensors to discriminate between intruders and nuisance alarm sources appears to be a fruitful area for further study.

Under contract 63-8967 with Sandia Laboratories, Adapt Service Corporation conducted studies on the effect of the intrusion scenario, field conditions, meteorological and environmental background on the performance of two types of intrusion detectors. The data analyzed was detection probability data obtained on three MAID flat and three MAID round intrusion detectors. In this study, the environment was defined by 518 independent variables including average spectra and a threshold crossing analysis for the wind velocity and direction, seismic background, acoustic background, and magnetic background. In addition to these continuous measurements, an additional fifty measurements were used to define the meteorological environment, the ground condition, and the intrusion scenario. Regression programs were used to relate each of the 518 independent variables to the observed detection probability. Pattern recognition analyses were also performed to separate environments for which the sensors had high detection probabilities from environments for which the sensors had poor detection probabilities. These were used to produce relative importance vectors to determine which of the independent variables were most important to the performance of the sensor. The specific conclusions reached by Adapt Service Corporation include the following:

(1) The environment had a significant effect on the performance of the six sensors studied. Specifically, the environment explains an average of approximately one-third of the variation in detection probability for these sensors.

(2) There was considerable difference between the amount of variation explained and the specific background and scenario measurements which explain this variation for each of the six sensors investigated.

---

(2) Evaluation of Fence Intrusion Detection Systems Op. Cit.

(3) All six of the sensors were similar in the fact that the dominant effect was due to one of the background measurements, although the specific background measurement varied from sensor to sensor.

(4) For these six sensors, the average seismic spectra occurring over the time period during which the sixteen runs occurred had no significant effect on the detection probability. It should be noted that the crossing analysis shows that the detailed variation of the seismic spectra during the sixteen runs does not have an effect on the detection probability for a number of sensors.

(5) Both regression and classification analysis lead to similar results for definition of the important background variables.

(6) Analysis of the correlation between the crossing variables suggests that less variables will be required to convey the information presented in the present crossing analysis.

(7) Sensor performance should be improved by proper correction for environmental effects.

(8) There were insufficient manned false alarm data in the present data set to allow adequate statistical analysis of the types performed in this study.

These data all suggest that there are indeed correlations between environmental background disturbances and sensor nuisance alarms, but that the current state of understanding regarding them is imperfect. Nevertheless, there is sufficient evidence to indicate that this is a promising area for further research. A reduction in nuisance alarm rates, which might be realized as a result of the collection and processing of appropriate background disturbance data, could have a significantly favorable impact on the performance of a CSSMRS that, over the long run, would justify a substantial research and development investment. Such an investment is recommended.

TASK 3. Consult with experts in the field of trace material detection to determine whether or not economical techniques exist for the detection of very low concentrations of some uniquely identifiable material which might be incorporated in the FEDS. Activation of FEDS would release this material and its detection would confirm activation and might support recovery actions initiated as a result of a successful attack/intrusion. Determine the requirements or potential for additional research in this area.

Findings: Consultation with personnel of the Analytical Chemistry Division, National Bureau of Standards, has revealed that there are several advanced techniques which might offer promise of detecting unique chemical materials in the extremely low concentration that might be involved in "tagging" an intruder into high security space.

Essentially, there are two types of tagging or labeling that can be contemplated. One is applied overtly as a constituent of a sprayed material which has characteristics that adversely impact one or more of the intruder's senses in ways which are calculated to deter his purposes. The trace material may be a particulate component that adheres to the intruder's clothing or body or a liquid or gas that is adsorbed by his skin. The other type of tagging may occur covertly and involve use of a colorless, odorless, and tasteless gas which might be ingested without the intruder's knowledge and which might be detected for periods ranging from hours to days later.

Candidate detection techniques for tracking or identifying these trace materials include gas analysis by absorption-fluorescence using lasers, optogalvanic spectroscopy, fluorescence spectroscopy of particles, and more remotely, artificial olfactory sensing.

The promise of these approaches was such that further research and development in this area was recommended and this recommendation was accepted and supported by DNA.

TASK 4. Evaluate the performance of currently available and emerging equipments for computer recognition of spoken words. This includes extent of vocabulary, speaker independence, and recognition probability. Typically, these equipments are designed as special "front-end" processors for attachment to a general-purpose minicomputer. It will be necessary to lease or purchase one or more units from the three known suppliers to complete the evaluation process. Assuming suitability is established, this equipment could be later incorporated in a prototype CSSMRS.

Findings: The potential application of automated speech recognition technology in CSSMRS involves the monitoring of guard forces communications channels, both radio and telephone, and interpreting verbal status reports to supplement information derived from the security system sensors. It might also be employed to verify the identity of guard forces personnel, and, in conjunction with an automated voice response system, it might be used to direct guards to make random patrol patterns.

The constraints on these potential applications that are imposed by the present state-of-the-art are quite severe. Continuous and semicontinuous speech understanding systems appear to be at least five to ten years in the future and to involve a level of data processing power and capability that would be difficult to justify.

Discrete word and phrase recognition systems appear to offer the best promise for potential use during the next three to five years. Over this period, it is anticipated that they will show useful advances in both vocabulary size and speaker independence, but even with these improvements their utility in the CSSMRS may be affected by a number of factors.

1. Guard forces may have to be trained to communicate using an artificial and highly restricted vocabulary in a rigidly constrained syntax. The effects of departure from prescribed communications format or from changes in voice characteristics in stress situation, such as the discovery of an intruder, could adversely affect system performance and must be fully and carefully evaluated.

2. It appears questionable whether total speaker independence will be available together with an adequate (although still limited) vocabulary before 1980, and, if this is the case, individual reference file vocabularies may be required for most, if not all, speakers. To date, a reasonable degree of speaker independence is only available in systems with a twelve-word vocabulary; the ten digits and "yes" and "no". Conceptually, these might be used to enter claimed speaker identity, and after verification, serve as the basis for selecting the appropriate reference file for that individual from the disk library. In a multi-speaker environment, the operational implications of such a procedure are not attractive and might be avoided if a speaker independent system with even a 50-word vocabulary can be developed within the appropriate time frame.

3. It is likely that a few individual speakers may experience difficulty with speech recognition systems on account of diplophonia or speech impediments.

4. The effects of band limiting, noise, cross talk, distortion, or interference introduced by the communications channel will influence the system error rates. Because of the high accuracy requirements of the CSSMRS, a voice repeat-back capability will probably be required to confirm that utterances have been correctly recognized by the system. This, in turn, will affect system response time. It is planned that these tests will be conducted in the near future using one of the commercially available word recognition units to obtain objective measures of the performance degradation that is expected to result from limiting the acoustic band width to values associated with a radio or telephone voice channel.

5. Pauses between words or phrases greatly facilitate word/phrase isolation and recognition but they adversely impact speed of communication and system response time.

6. System redundancy would be required for the recognition of speech occurring simultaneously on more than one communications channel. Conceptually, more than one channel can be combined to provide a single input to the speech recognition system provided only one channel is active at a time. However, restricting communications to sequential, one at a time, activity on multiple radio and telephone channels may well be operationally intolerable.

These considerations suggest that plans to incorporate voice recognition equipment in the CSSMRS should proceed with caution. Progress is being made in improving the capabilities of voice recognition systems but it has not occurred as rapidly as was forecast. It could undoubtedly be accelerated by the initiation of research and development efforts specifically oriented toward producing a speech recognition system capable of meeting an acceptable subset of the CSSMRS objectives. It is believed that these would require that such a system should have at least the following capabilities:

a. A vocabulary of at least 25 and preferably 50 words or phrases.

b. Recognition accuracy of at least 98 percent operating in real-time and with no more than 0.1 second separation required between words or phrases.

c. Above accuracy to be attained from at least none out of ten native born American speakers selected from the population at random, and without requiring the use of individual speaker reference files or prompt the repetition of utterances.

d. A voice response capability to verify recognition accuracy or prompt the repetition of utterances.

e. Computer understanding of the meaning of certain key phrases or sentences.

f. A capability to verify the personal identity of up to at least 20 speakers.

Pending the development and availability of a system having these "acceptable" capabilities, it is believed that some utility might be derived from systems which might be currently available by using a highly restricted vocabulary and rigidly constrained communications protocol with numerical encoding.

The vocabulary would be restricted to twelve words, the ten digits and "yes" and "no". No speaker independence is assumed and initial system training would involve use of two-digit numbers uniquely assigned to each member of the guard force. These would serve a dual purpose; to confirm the identity of the individual and to call up the reference twelve-digit vocabulary for that individual from the file. Subsequent communication would take place in a digitally coded format; for example, a two- to four-digit preamble group, representing status, password or duress word, followed by a four-digit group representing time of day. Use of a four-digit preamble group could provide a basis for adding a slight measure of additional security to passwords or duress words. For instance, any four-digit preamble where digits two and four were odd could be designated as a duress word on a given day. Numerous other easy to remember coding schemes can be visualized.

The use of a word recognition system of even this reduced capacity is dependent on the outcome of tests on the effects of band limiting noted in item (4) above, as well as satisfactory resolution of the other limitations and constraints that have been identified. Its inclusion in CSSMRS cannot be fully endorsed at this time; rather, it remains an item for further consideration.

TASK 5. Review current security manuals and visit one or more secure sites to collect detailed information on security operating procedures, voice communication protocols and response initiatives. Assess and evaluate changes that might be desirable or necessary as a result of implementation of the CSSMRS.

Findings: Site visits have been made to one Army, one Navy, and one Air Force site. The principal comments developed as a result of these visits are as follows:

General Comments

The guard forces seem adequate; indications are that they would respond quickly and vigorously once an intrusion has been detected. The acreage outside the limited area is swept occasionally by the security forces so it would probably be hard to tunnel in or construct an attack base near the perimeter.

The chief concern expressed by nearly everyone is the possible defection of personnel. Also high on the list of concerns is the relatively high vulnerability of the weapons when they are being moved and some dissatisfaction with presently available guard communications both on base and in transit.

What happens when there is a fire inside the limited area is not clear. There is always a branch of the base fire department not far from the entrance but the only access control procedure we were told of is that the number of firemen leaving is checked against the number admitted; however, specially trained firemen (nuclear qualified) are always under the direct observation of the security forces while they are in the exclusion area.

Department of Defense Directive 5210.42 prescribes the limits of access to weapons that are permitted to properly cleared security forces. Within these constraints, it is recommended that CCTV cameras be used inside the magazines for assessing the validity of alarms. The desirable objective of not permitting the guards to have knowledge of the contents of a storage magazine could be maintained in the presence of the recommended interior CCTV surveillance capability by shrouding weapons or other magazine contents with opaque sheets of cloth or plastic. The CSSMRS could easily be programmed so that the CCTV system within a magazine is automatically disabled when the magazine is in the "access" mode. This would prevent guard forces from observing the magazine contents when

workers are present and one or more shrouds has been removed. The advantages of having positive alarm verification or refutation by means of CCTV or other assessment means would appear to overwhelmingly outweigh the minor inconvenience of handling shrouding.

In all cases, appropriate lighting will be necessary in order to use CCTV. If adopted, the sodium vapor lighting system that is being considered should be adequate for the use of outdoor CCTV. Alternatively, low light level camera equipment could probably be used with existing lighting supplemented by some controllable spot lights. Appropriate combinations of fixed and pan/tilt/zoom cameras should contribute significantly to enhanced perimeter security.

The radio communications system needs to be dramatically improved if CSSMRS is to include voice recognition equipment. Operators need to be trained to follow more disciplined procedures. The training problem is complicated by the fact that the guards are constantly rotated with the large base security force. This fact will no doubt impact other systems as well since it increases problems in identification, screening, training for special procedure, etc.

There has to be a secure location for installing the CSSMRS central computer and related hardware. It is not known if the new Alarm Control Center (ACC) building will have suitable space available or not. No such space was evident in the facilities we visited.

The following are areas seen as presently weak that would benefit from CSSMRS:

Key accountability

Duress alarms for sentries and workers in the bunkers (none at present)

Local alarms for bunkers

Positive identification of the guard calling in from a bunker.

TASK 6. Develop a comprehensive series of intrusion/attack scenarios and formulate optimal CSSMRS responses. This will require liaison and coordination with recognized experts in the physical security community.

Results: The development of intrusion/attack scenarios is a difficult but potentially very rewarding task. It is difficult because an imaginative or ingenious scenario is required to truly test the contemplated physical security measures, but at the same time, the scenario must reflect a creditable threat; one that will not be dismissed out of hand. To the extent that these two conflicting objectives can be reconciled, scenario development is rewarding through the insight that can be provided regarding the attributes that the security system must possess in order to be effective against the postulated threat. These attributes include the identification of types of sensors that would be useful. Some of these sensor types are not currently installed members of the present family of physical security sensors. The credibility of the threat which they would provide protection against might be a measure of the urgency of the need for their development, test, and evaluation. Other desirable system attributes that have been identified through the examination of intrusion/attack scenarios include the use of a variety of forced entry deterrents (FEDS), the use of closed-circuit television for rapid and positive alarm verification, and the establishment of at least a preliminary list of circumstances that appear to justify the immediate and automatic call for assistance from backup or reserve forces.

In the development of these scenarios, it has been assumed that the threat may involve as many as ten or fifteen, or as few as only one or two dedicated, well-trained individuals who are not particularly limited by financial or technical resources and are free to wait and to time their attack to coincide with the occurrence of a preselected set of conditions, such as weather, time-of-day, etc.

A number of scenarios were developed. Their details are censored and are unpublished to avoid classification of this report. Only the CSSMRS attributes or characteristics which were revealed as a result of the study of these scenarios are listed as Task 6 findings. These include the following:

1. CSSMRS must have provision for the guard force to acknowledge every alarm.

2. The guard acknowledgment of each alarm must occur with a fixed limited amount of time; fifteen to thirty seconds is suggested. If this time is exceeded, CSSMRS should initiate an alerting message to higher headquarters.

3. Any alerting message to higher headquarters should cause them to issue an immediate authentication request. The response to this request will serve to guide subsequent action. If voice communication is used for this request, confirmation by two members of the guard force should be required to protect against a defecting individual guard. A negative or no response should be cause for immediate dispatch of backup forces.

4. Backup forces should be dispatched in multiple vehicles and should be equipped for any eventuality including poison gases.

5. When any sequence of alarms occurs that are indicative of a progressive intrusion, and when no acknowledgment has been made of these, an automatic call for backup forces should be made within 10 seconds of initiation of the second alarm.

6. In addition to other circumstances yet to be defined, FEDS should always be armed whenever there is a call for backup forces.

7. Following any call for backup forces, CSSMRS should make immediate up-channel reports of all events that are sensed.

8. Magazine ventilators could be equipped with break-wires or other sensors that would cause an alarm if the cover were removed or if an object were inserted to attack the inner protective grill.

9. Fire-fighting systems which could be activated from outside a magazine without opening the doors would help to counter the threat of this scenario. These might be in the form of standpipes equipped with sprinkler heads through which carbon dioxide, form or other appropriate agents could be pumped into a locked magazine.

10. Point sensors that would detect the removal of any individual weapon would provide added protection against substitution of a dummy duplicate. Placing these sensors in access mode should be independent of other intrusion sensors.

11. Reduce the cross sectional area of magazine ventilators so as to maximize the length of time that vapor type FEDS will be effective.

12. Consideration should also be given to the advisability of locating a portion of the FEDS release points immediately adjacent to or perhaps even under the individual weapons with arrangements so that these could be triggered when point sensors showed that the weapon was being touched or moved by an intruder. This capability would be disabled by means of suitable safe/arm mechanisms at any time the magazine was in the "Access" mode.

13. Successful development and integration of a sensor which will detect parachutists that intrude the air space over a site is recommended.

14. The CSSMRS central computer should be provided with a sensor to detect radio jamming of the guard forces' communications system.

TASK 7. Develop estimates of computer speed, work load, core and storage requirements which the CSSMRS will require.

Findings: The CSSMRS concepts have evolved toward a distributed process where a number of remote microprocessors are interconnected to a central station processor, which, in turn, is in communication with backup and reserve forces. In developing estimates of the capabilities that each of these types of processors will require, it is useful to list the principal tasks that each will be expected to perform.

Each remote microprocessor will be concerned with all aspects of a limited physical area, such as a single storage magazine of a few segments of the perimeter zone. In this capacity, it will be required to do at least the following:

(1) Measure elapsed time.

(2) Monitor the output of its local group of sensors.

(3) Report status to central processor in response to poll message.

(4) Report sensor alarms to central processor.

(5) Test sensors periodically.

(6) Accept Normal/Access status commands from central processor.

(7) Accept FEDS Safe/Arm/Actuate commands from central processor.

(8) Confirm communications integrity with central processor.

(9) Assume autonomous mode of operation if communications with central processor fails.

(10) Accept some weather information from central processor and do limited correlation with sensor outputs.

(11) Operate CCTV controls under commands from central processor and disable CCTV when mode is "Access."

(12) Assume all related and subsidiary tasks inferred by the above list.

This list does not represent a particularly heavy processor work load and thus processor speed requirements are not severe. Much more important are high reliability, tolerance to wide temperature extremes and low power consumption. A Complimentary Metal Oxide Semiconductor (CMOS) family of microprocessor products is currently a strong candidate for the application. It is capable of operation over the temperature range of -55 degrees to +125 degrees celsius, and it tolerates a considerable variation in power supply voltage. Typical instruction times range from 2.5 to 3.7 microseconds, and at this speed the CPU power consumption is only 50 milliwatts. It is estimated that 1 K bytes of random access memory (RAM) and 8 K bytes of read-only memory (ROM) might be required for each remote microprocessor.

At the central station, the processor will be required to do at least the following:

(1) Measure elapsed time.

(2) Maintain a time-of-day clock.

(3) Collect environmental background data. Candidate items include wind speed and direction, visibility, precipitation, temperature, lightning, magnetic and seismic data.

(4) Poll each remote microprocess in turn and accept status reports.

(5) Be interrupted by, and accept alarm messages from remote microprocessors.

(6) Correlate sensor alarms and environmental background disturbances.

(7) Drive displays and operator's console showing security status.

(8) Monitor guard responses to alarm conditions and make appropriate up-channel reports.

(9) Send and keep track of Access/Normal status and FEDS Safe/Arm/Actuate commands and CCTV commands for each remote microprocessor location.

(10) Monitor communications integrity to remote microprocessors and to higher headquarters.

(11) Provide dual language operator console or audible instructions as required in overseas areas.

(12) Monitor trace material detectors.

(13) Monitor word recognition system (if used).

(14) Monitor radio jamming detector.

(15) Generate tasks for guards, randomize patrols and authentications.

(16) Monitor guard activity and duress sensors.

(17) Authenticate claimed personal identity.

(18) Other related and subsidiary tasks implied by the above list.

This list represents a rather substantial basic work load for even a small site. Above this basic load, the work increases in a more or less linear fashion as the number of remote microprocessors increase with the size of the site. At present, the undefined and undefinable extent of some of these tasks, notably (3) and (6), make it impossible to say with certainty whether or not all of these tasks can even be accomplished with anything but a multiprocessor environment. Certainly (13), and probably (18), will require a special-purpose pre-processor. Excluding the work load reflected in these four tasks, it is estimated that the remaining functions could be accomplished using a moderately fast minicomputer equipped with 256 K bytes of non-volatile memory, perhaps magnetic bubble, for word generation, and 32 K bytes each of ROM and RAM. Because of the critical nature of the central station processor functions, this should be a dual, fully redundant system arranged so that the backup processor would automatically take over in the event of any failure in the primary processor. Depending upon the ultimate resolution of the nature of the tasks in items (3), (6), (13), and (18), it might be possible that some or all of these tasks could ordinarily be handled in the backup processor and that some or all of them could be temporarily dropped during any time that the backup processor was required to assume primary control.

TASK 8. Collect information on the types of computer equipment which may already be installed at sites and their suitability from both hardware and software standpoint to support the CSSMRS.

Findings: The CSSMRS application puts a particularly high set of requirements on its computer complement. If the system is to be of any help to the guard forces, it must be trustworthy in fact as well as appearance. It will not be accepted by the men in the field if its actions do not inspire confidence. Expressed in a more technical manner, a computer used for security monitoring and response initiation must have certain attributes as follows:

(1) It must be highly reliable. Any significant down-time will be intolerable.

(2) It must be highly secure. The installation defense plan will be (at least partially) contained in the response initiation software. The intrusion detection software should not be compromised to deter evasion and harrassment.

(3) It must have predictable response characteristics. When a given set of security conditions prevail, the computer response time must be acceptable.

The effects of time-shared operation will now be evaluated in light of these requirements.

[1] High Hardware Reliability. Unfortunately, the hardware failure rate of electronic equipment, including computers, becomes worse as size and complexity increases. Thus the use of a large, time-shared computer will result in more frequent down-time caused by hardware failure. Of course, redundancy and error correction techniques can be added to a large computer, but they themselves are subject to failure and can be even more effective when applied to a basically more reliable smaller system. Highly reliable commercial systems usually have nightly or weekly slack periods in which down-time can be scheduled. Scheduled down-time in a CSSMRS installation would probably require the mobilization of reserve forces to patrol the installation perimeter during the outage. Any computer system used for security monitoring and automatic response initiation must be provided with backup power source to operate the system for a number of hours in the event of commercial power failure. A small dedicated system could probably be economically carried by a battery backup supply,

which would be more reliable than an independent engine-powered a.c. generator.

[2] Software Reliability. It has been stated that no program of over 1,000 statements is known to be absolutely perfect and correct. While many much larger programs are successfully in use in applications requiring high stability and reliability (such as airline reservations systems), the fact remains that software complexity reduces the confidence in the correctness of operation. The airline computer is under the direct control of the user who requires reliable performance, rather than an outside organization as would be the case if the CSSMRS system were time-shared of a host computer belonging to others.

Operating systems for large time-shared computers generally consist of tens of thousands of statements. Much less system software is required with a dedicated computer. If time-shared operation is required, a full study and considerable software modification will be required for each type and configuration of the host computer. This will greatly expand the software effort required to insure a reliable system.

[3] Software Security. The present state-of-the-art in time-shared operating systems is such that the major goal is to increase the interval between system "crashes", and security is a secondary consideration. One of the banes of multi-user time-shared computers is data and program security. The problem of keeping one user out of another's area is not easy as evidenced by the experience of university time-sharing systems. While students may have a natural inclination to attempt to beat the system, anything that the student can do intentionally will happen sooner or later because of operator or user carelessness. Conventional time-shared computers do not provide hard-wired (not programmable) hardware security to restrict use of the portion of memory containing the software to "execution only". This may be required to prevent the program from being used as data and being listed out by an intruder or inside accomplice for later analysis.

Virtual memory, a common money-saving technique in modern time-shared systems, results in programs and data being swapped in and out of memory frequently during pauses in execution. Generally the

swapping-in is to a different portion of memory each time. Fragments of a program and its data will remain in working memory each time it is swapped out. This forms a means of getting another user's program.

[4] Unpredictable Response Time. The sizing of time-shared computers is generally done to accommodate predicted demand with a reasonable response time. The problem is that prediction of demand is not easy. With many users, each of which has a large peak-to-average ratio in demand, the computer will appear to be under-utilized most of the time if it is large enough to handle peak loads without long delays. There remains the problem that the other users of the system may have regular requirements which monopolize the machine to the extent that it will not be able to give adequate service to the security system for minutes at a time. If an intruder intended to attack a base in which the security program operated on a time-shared system, he would surely attempt to overload the computer system by inspiring a peak load from the other users at the critical time. Of course, the system will be unavailable for an extended period should computer-operating system modification or updating happen, even if the changes are not made in the portion of the software which is directly used by the security system.

The foregoing considerations lead to the inescapable conclusion that attempting to time-share a security system on a computer with other users would result in a totally unacceptable level of performance.

Section II

System Description

The Computerized Site Security Monitor and Response System (CSSMRS) was originally visualized as a network in which all site security systems, including intrusion detection equipment, intrusion deterrent systems, duress alarms, guard radio and telephone systems, meteorological or environmental background sensors, and off-site interdiction and recovery sensors, and Backup or Reserve Forces are interfaced to a computer to provide timely, accurate and unambiguous information about the progress of an attack or intrusion attempt and the programmed decision of how best to counter it. Automatic up-channel status reports would signal any change in site security status and the response actions being initiated. These programmed responses could only be countermanded by order from a higher connected command echelon.

This section of the report provides a current but incomplete description of the CSSMRS. It identifies some of the alternative choices which must be considered and discusses some of the trade-offs that must be resolved to permit final definition and specification of the CSSMRS.

During Phase I, the specific tasks described in Section I of this report were addressed and the findings resulting from that work have influenced the evolving CSSMRS concepts in a number of ways. Perhaps one of the more significant of these results from recognition of the advantages of a distributed network of processors as contrasted to the centralization of all system control. Each magazine or bunker would be equipped with an appropriate complement of sensors, forced entry deterrent system (FEDS), an intrusion alarm, and a closed-circuit television system with pan/tilt/zoom controls all interfaced to a microprocessor, which, in turn, is in communication with the CSSMRS central processor. Figure 2 is a simplified block diagram showing the proposed arrangement.

Inputs to the microprocessor are sensor alarm signals, status indications from two levels of safe/arm switches, sensor tamper switches, and power failure. Outputs include CCTV camera and lighting controls, intrusion alarm sensor test facilities, access/normal controls, control of a local audible alarm, and the arming and firing of FEDS. Under ordinary circumstances this complex would function as a slave or satellite station accepting commands from the central CSSMRS processor and responding in the manner in which it was directed. Should an intrusion alarm condition occur, the microprocessor at the magazine would immediately notify the central CSSMRS processor, actuate the local audible alarm, and electronically arm the FEDS. This would permit subsequent firing of the FEDS so long as the series connected manual safe/arm switch was also in the "arm" position. Normally, the central

SIMPLIFIED BLOCK DIAGRAM OF STORAGE MAGAZINE CONFIGURATION

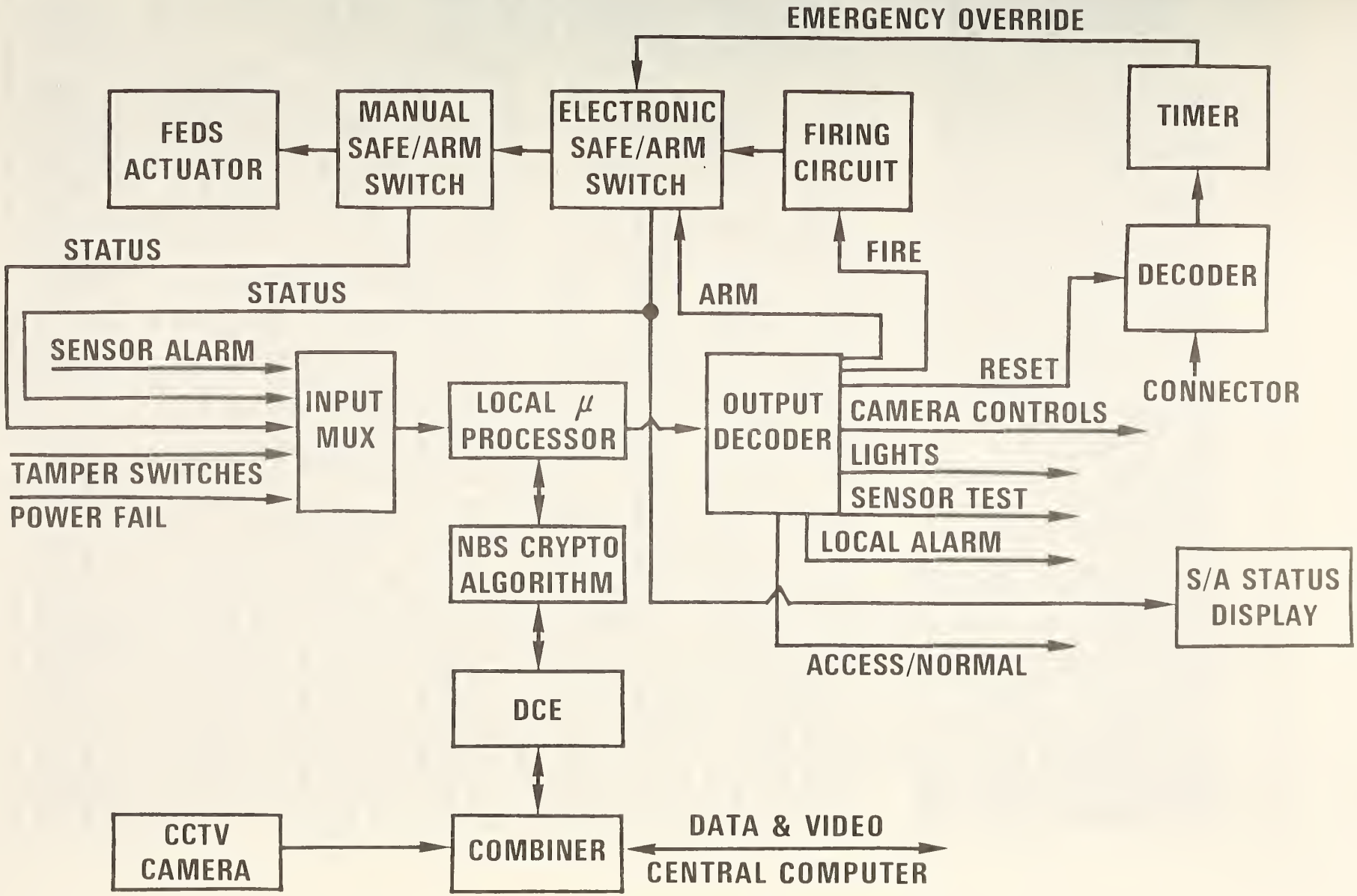


FIGURE 2

processor would immediately acknowledge the alarm message. This would then be followed by additional messages initiated by the guard that would (1) activate the interior lights, and (2) connect the CCTV system to the guard's display at the central station, and (3) would inhibit the actuation of the FEDS until the guard could determine the validity of the alarm condition using the remote pan/tilt/zoom CCTV camera controls. If visual examination confirms the presence of intruders or any other abnormal threat to the restricted area, the guard would direct patrol forces to the site by radio and he could optionally also actuate the FEDS. If visual examination discloses that a nuisance alarm had occurred, the guard at the Central station could reset the sensor and silence the local alarm and also extinguish the interior lights and release the CCTV system.

At this point some discussion of contingencies and alternatives is in order. In the foregoing it has been assumed that all electronic systems and the guard force are functioning normally. Under actual intrusion/attack circumstances this might not necessarily hold true and the CSSMRS must be arranged to cope, to the greatest extent feasible, with such eventualities. Assume, for example, that the communications link from the storage magazine to the CSSMRS central processor has been broken or that the CSSMRS central processor has been disabled. Failure of the magazine microprocessor to receive an immediate computer-generated acknowledgment to its alarm message would constitute evidence of such a problem. Under these circumstances, the magazine microprocessor should revert to an autonomous mode of operation. It should continue to sound the local alarm for one minute and then, if the intrusion alarm condition persisted, the FEDS should be activated.

The rationale for continuing to sound the alarm and delaying the activation of the FEDS for one minute when communication with the central processor is lost is to accommodate a unique situation that might otherwise endanger authorized workers in a magazine. Access/normal mode in a magazine will be set as a result of a command from the central processor. An "access" command must be continuously reiterated at regular intervals to insure its authenticity and continuity. In other words, a fail-safe philosophy demands an automatic return to "normal" mode as a result of expiration of a time limited "access" mode command. Authorized workers entering a magazine which has been placed in the "access" mode would immediately unlock (using a key) and manually operate a FEDS safe/arm switch and set it to the "safe" position. This would make it impossible for the FEDS to be activated as a result of system failure or any related accident. Assume, however, that a communications link or CSSMRS central processor failure should occur after the "access" mode had been set in a magazine but before the manual FEDS safe/arm switch had been set to "safe." The expiration of the "access" time limit would cause the mode to revert to "normal." An open magazine door and/or the presence of workers inside the magazine would cause an alarm condition. The local alarm would sound and this, coupled with the one-minute delay in FEDS activation, would alert the workers to provide time for them to either (a) evacuate the area and eliminate the

conditions causing the alarm, or (b) actuate the safe/arm switch to the "safe" position.

In the case of a tamper alarm at the magazine, the sequence of events might be somewhat different since it is anticipated that tamper alarms would be associated with certain components of the system which might be physically located in a tamper-resistant container outside the protected magazine. Here the appropriate message would be transmitted to the central processor without activating the local alarm. The idea would be to avoid alerting the tamperer that he had been detected and to dispatch a guard patrol to apprehend him in the act. Here again, however, if the tamper alarm message is not immediately acknowledged by the central processor, it is an indication of a problem; perhaps the communication link has been cut by the tamperer. Under these circumstances the magazine microprocessor should revert to the autonomous mode of operation and immediately activate the local audible alarm.

The occurrence of either a tamper alarm or an intrusion alarm should require an affirmative acknowledgment action on the part of the guard on duty at the central station. If the required guard acknowledgment does not occur within 30 seconds, this should be considered as evidence of possible incapacity on the part of the central station guard and the CSSMRS central processor should automatically initiate a message to higher headquarters requesting backup reserve forces.

Referring again to figure 2, there is a connector, decoder, and timer associated with an emergency override feature on the electronic safe/arm circuit of the FEDS. This feature is intended to provide an emergency mechanism that could be invoked in the event of failure or malfunction of CSSMRS components within the magazine so as to provide authorized access for repair without compromising the security of the magazine. The "key" to this emergency override circuit is an electronic module which is kept in a safe by the base security officer or other designated responsible officer. When this module is plugged into the override connector at the magazine, the local audible alarm is sounded. The module produces a bit pattern which must be recognized by the decoder. If the bit pattern is successfully recognized, the audible alarm is silenced and the timer is started. At the expiration of a timer interval that has been preset in both the timer and the "key" module, a gating window is established which permits the transmission of another bit pattern from the "key" module to the electronic safe/arm switch. The successful gating and recognition of this pattern will set the switch to the "safe" condition which will be displayed on the S/A status display shown in figure 2. Failure to recognize the second coded bit pattern, or its occurrence at a time other than the proper gating window, will reset the timer and reactuate the audible local alarm.

Under normal circumstances, the CSSMRS central processor would poll each microprocessor in the distributed complex in sequence. This poll message would confirm to each microprocessor that the central processor and its data link were functional. It would revalidate any currently

outstanding "access" mode commands and inhibit the transition of each affected microprocessor to the autonomous mode of operation. The normal reply to this poll message would be a status report indicating the condition of all system components with which the addressed microprocessor is concerned. The initial report of any alarm condition would be made by a microprocessor immediately and not deferred until receipt of the next poll message, but a continuing alarm condition would be reaffirmed in response to each round of polls. Given this mode of operation, the question of polling frequency must be considered. The polling should be often enough that there would be no uncertainty regarding the status at any magazine for an unacceptably long period of time, but the sequence should not be so frequent as to cause an undue work load on the central processor. An interval of 10 to 15 minutes is suggested. This time interval is small compared to the typical useful life of the standby battery power supplies that would be required during a power outage so maintenance action to correct loss of primary power could be initiated with adequate promptness. Also, it is assumed that the duration of any "access" mode condition would probably have to be at least 10 to 15 minutes long and that this might be an appropriate "access" revalidation interval.

One might advance as an argument for a shorter polling interval an assumed attack/intrusion scenario in which the restricted area (but not the magazine) has been penetrated without tripping the perimeter alarms. Assume further that the intruders, perhaps with the assistance of a defecting guard, have knowledge regarding the start of each polling cycle and cut the data link immediately after a polling cycle has been completed. Under these circumstances, there would normally be a delay equal to the duration of the polling interval before the central processor had positive indication that the communications capabilities were impaired. If, during this interval, the intruders penetrated a magazine or tripped a tamper alarm, the failure of the magazine microprocessor to receive an immediate acknowledgment to its alarm message would cause it to go to the autonomous mode of operation and to activate the audible local alarm. The audible local alarm would be interpreted as a signal for guard patrol forces to converge. If magazine penetration had occurred and persisted for one minute, the FEDS would be activated releasing unique trace materials. These trace materials would be detected and this detection would be the basis for the central processor to automatically dispatch a message up-channel calling for backup reserve forces. It is concluded that even this scenario does not justify a polling interval shorter than 10 to 15 minutes.

The physical location and housing arrangements for the remote microprocessors are another matter for consideration. If the potential security benefits of the FEDS are to be realized, then it is vital that the link between the microprocessor and the FEDS be highly secure. After all, the chief contribution of the FEDS is visualized as resulting from their deterrant/delay potential which might buy time for the arrival of backup forces in the event of total incapacitation of the local guards. If the microprocessor controlling the activation of the FEDS were located and housed in such a manner that an adversary could successfully

cut the firing command link to the FEDS, their potential utility could be completely negated.

If the microprocessor were located within the protected magazine, it could be safely contained within a simple protective housing as it would then be guarded by the same intrusion alarms and sensors that protected the magazine itself. This arrangement would probably be the most secure, but it has the obvious disadvantage that access to the magazine would be required in order to perform preventive or corrective maintenance actions.

An alternative arrangement would be to house the microprocessor in a vault-like cubicle or housing attached to the outside of the magazine. If this arrangement were chosen, it would be necessary to protect this enclosure with intrusion detectors, and to construct it with sufficient strength and integrity to offer promise that its penetration resistance time would approximate the response time of the backup forces. Even with these precautions the potential vulnerability in the face of a determined attack would be much greater than if it were located within the magazine in a simple housing protected by an ordinary tamper-switch on the access door.

In addition to the greater security that would result from locating the microprocessor within the magazine, it is expected that this location would contribute to greater system reliability since the environmental conditions within an earth-covered magazine would not be subject to as wide a variation as those in an external cubicle.

In all of the foregoing description, the microprocessors have been associated with a group of sensors in a magazine; however, most of the same concepts are also applicable to a group of perimeter sensors. For example, a microprocessor might be interfaced to from one to five 100-meter segments of in-depth perimeter sensors and security components, together with a CCTV camera which could be used to inspect that portion of the perimeter. In such an application, the camera should probably be mounted on top of a low tower or pole and inside of a tamper and weather-resistant enclosure. A tower or pole would be located at about the center of a 100-meter perimeter alarm segment and the camera would be aligned to monitor the N subsequent segments to the right of the segment in which it is located, where N is determined by terrain, perimeter meander, and any other factors influencing visibility. In this way each camera would always be pointed in approximately the right direction to cover its segments of interest to facilitate capturing short duration events. Pan/tilt controllability could be either severely restricted in range or perhaps eliminated entirely. The camera would be recessed within its enclosure far enough that this, together with the height of its mounting, would make it difficult to obscure the field of view by paint spray or other objects. Polling, status reporting, and alarm reporting would all take place in the same manner as in the magazines. Sensor testing would probably best be accomplished by the CSSMRS central processor randomly selecting perimeter segments to be walk-tested and presenting these selections to the central station guard

who would, in turn, direct the roving guard patrols accordingly. This would be in contrast to the routine testing of the magazine sensors (except CCTV) which would normally be done automatically without the participation of guard patrols. Testing of all CCTV systems would require the support of the central station guard that was on duty, who would activate lights if required and would exercise pan/tilt/zoom controls to ascertain that each camera was functioning properly. Note that the CCTV camera would be automatically disabled in an area in the access mode and that all testing would be inhibited during these periods.

The recommended approach to routine testing is to exercise the components associated with a different microprocessor during the interval between each routine polling sequence, typically alternating between a magazine and a perimeter microprocessor. With the suggested polling interval of 15 minutes, this would test four locations per hour and would cover all systems on a large site at least once per day. This procedure would provide a steady flow of tasks for the guard forces to accomplish as well as helping to randomize guard patrol movements.

At this point some discussion is in order about the communications link between the various microprocessors and CCTV cameras located in the several magazines and the designated sections of perimeter around the storage site and the CSSMRS central processor and guard's display. This communications link must have a relatively broad bandwidth capability since it must handle both video from the CCTV as well as digital data. For the moment, the question of the number of simultaneous video channels that it must handle is left open. The link must be highly reliable as it is one of the key components in the CSSMRS, and it must be secure since the introduction of a false and invalid "access" command might negate the security of the entire system.

There are two media that are principal candidates for use in providing this link; coaxial cable and fiber optics. Each of these offers both advantages and disadvantages.

Coaxial cable has the following advantages:

(1) The technology is well known and established. Components, such as cables, connectors, amplifiers, combiners, splitters, etc., are highly developed and readily available.

(2) It is readily usable in a multipoint configuration, i.e., many stations can be tapped off a single length of cable.

(3) A single cable can be used for two-way simultaneous transmission.

(4) It is less expensive than fiber optics.

Its disadvantages include the following:

(1) It can be tapped, i.e., some form of line supervision or cryptography would be required to insure the integrity of data communications and eliminate any possibility of an intruder inserting an unauthorized "access" command.

(2) It is not completely immune to interference from electromagnetic sources, such as lightning or other intense sources of RFI.

The advantages of fiber optics include the following:

(1) It is immune to any form of electrical or radio frequency interference.

(2) It is relatively secure; it cannot be easily tapped, and it would be quite difficult to break the link and insert false data as a substitute for authorized CSSMRS messages. These characteristics would probably make it unnecessary to use cryptographic techniques to insure the integrity of the data link.

The disadvantages of fiber optics include:

(1) A fiber optic link is most efficient as a unidirectional point-to-point channel. For multipoint configurations, power splitters are available that will typically divide the incident input power evenly among several output ports with a net loss on the order of 2 dB over and above the division factor. That is, the sum of the output power at all ports is only about 2 dB less than the input power. Since only small amounts of power can be injected into an optical fiber from a diode laser, fairly frequent regenerative repeaters are required in conjunction with power division to maintain an adequate signal-to-noise ratio in a multipoint configuration. An arrangement of this sort is unidirectional and a complimentary configuration is required for the return path. The dispersion introduced by these power splitters and its resultant effect on bandwidth must be determined in order for this technique to be fully evaluated. The alternative is to run a separate pair of fibers between each microprocessor and the central CSSMRS processor. This would require up to 100 receivers at the central processor as compared to only as many receivers as there would be simultaneous video channels if coaxial cable were used.

(2) The technology is new and there is a rather limited selection of components that are presently available.

(3) The cost of low loss fiber optic cable is currently about $3.00 per meter in large quantities. The installed cost of a fiber optic link would probably be somewhat greater than one using coaxial cable. This cost differential is expected to diminish rapidly with the passage of time.

A further possibility that must be considered and evaluated in selecting the communication media is the use of both coaxial cable and fiber optics; coaxial cable for the video data from the CCTV and fiber optics for the digital data flow between microprocessors and the central processors. Such a hybrid arrangement would allow the use of readily available and relatively inexpensive CCTV components that have been developed for use in cable TV application, and, at the same time, the reduced bandwidth that would be required on the fiber optic link to handle only the digital data would permit the use of slower and less costly diode lasers and photodetectors. These potential savings would be offset to an as yet undetermined extent by the added costs of the dual media.

Further study must be given to these techniques before a final selection can be made; however, fiber optic technology is advancing and appears destined to become one of the major communications media of the future. In November 1976 the International Electrotechnical Commission (IEC) decided, at a meeting held in Geneva, to accept a proposal that it begin work on international standards covering the field of fiber optics applied to telecommunications apparatus and components.

Sensors that are interfaced to the remote microprocessors have only been treated as generalities. While the selection may vary, it is believed that the minimum complement for a magazine should include the functional equivalent of magnetic switches on the doors and on the ventilator cover, vibration sensors which would respond to efforts to penetrate the concrete shell of the magazine, and motion detectors that would respond to any movement within the magazine. Additional desirable sensors include point contact sensors which would respond to any movement of an individual weapon.

Sensors which would be interfaced directly to the CSSMRS central processor include those for sampling the environmental background to provide correlation data for aiding in the identification of nuisance alarms, the detector for the unique trace material contained in the FEDS, the detectors for an airborne intrusion, radio jamming, guard force activity and duress sensors, and tamper alarms. A word-recognition system would also interface with the central processor at such time as capabilities in this area have been developed to the point where the performance would be useful. Personal identity verification devices,

such as those being developed under the Base and Installation Security System (BISS) program, generally function with a stand-alone processor, but the output of this processor would be expected to be delivered to the CSSMRS central processor.

Up-channel communication between the CSSMRS processor and higher headquarters should be accomplished using a redundant data link with alternate routing so that communications capability could not be lost as a result of any single link malfunction or outage. Serious consideration should be given to the use of a satellite link as one of the alternate routes for message exchange with higher headquarters. There have been steady reductions in the size, cost, and complexity of ground stations for use with geostationary satellites. Such a ground station could be located within the restricted area and would be less accessible to an adversary than a hard-wired land line running through the countryside and would probably be less costly than a terrestrial microwave link. Both a terrestrial and satellite radio link are subject to disruption by jamming, but there is a higher level of skill, expertise and equipment that is required to jam than is required to cut a land line. In addition, certain types of jamming could be readily detected and that in itself might be considered as an indication of threat and a basis for response actions. It is anticipated that NSA crypto equipment and procedures would be employed on any type of data link to insure the security and integrity of information transfer.

The CSSMRS central processor complex itself should be fully redundant with a hot backup ready to take over in the event of failure of the primary processor. It, together with its uninterruptible power supply should be housed in a secure location or vault that is equipped with intrusion and tamper alarms. Processor memory is a particularly critical item; it should be non-volatile and not involve mechanical moving parts. Magnetic core and bubble memories and static ROMs appear to be the most viable candidates for this application. Application programs should be contained in ROM and the processor should be arranged so that the ROM contents could only be executed and not output as data. This feature would contribute greatly to the security of the software.

The controls and displays for the central station guard should be simple to understand, unambiguous in meaning, and easy to operate. One way of displaying overall security status of a site is by means of a pictorial or map-like representation of the site where color-coded status signals indicate which buildings or magazines are in access mode, and which of these and which perimeter segments are in the normal (secure) or alarm states, and other indicators showing if any sensors are inoperative or functioning on backup power supplies. Such a display panel might be in the form of a scaled-drawing or perhaps an orthophoto of the site that depicts all features that might have significance from a security standpoint. Each building should be numbered as is each segment of the perimeter alarm system. Lamps should be associated with each numbered element to indicate its status. Red flashing when an alarm occurs, changing to steady red when the alarm is acknowledged;

amber when any structure is in "access" condition. A single green lamp will be illuminated when ALL areas are secure, i.e., no structures in "access," no alarm conditions, and no sensors operating on battery backup power or inoperative; otherwise a white light is on.

In a number of respects this display panel is similar in function to the Area Display Unit (ADU) of the Base and Installation Security System. It differs in concept in that all display lamps (LEDs) would be controlled by a microprocessor associated with the panel rather than by hard-wired logic units. This microprocessor would be in continuous communication with the CSSMRS central processor from which it would receive the necessary status information to control the displays. Such a configuration would permit any alarm condition or other change of status to be displayed within a few milliseconds after it had occurred.

Any alternative status display arrangement would involve the use of a color cathode ray tube display. As with the map-board configuration, the site plan would be continuously displayed and status changes could be indicated by appropriate color changes. This sort of arrangement could also offer a potential capability to shift the field-of-view and examine a selected area on an expanded scale. It, too, would be under control of a microprocessor, and either approach would permit replication of the status display at multiple remote locations.

Associated with either type of overall status display is a monochrome alphanumeric (CRT or plasma) message display unit that provides more detailed information about conditions indicated on the status display.

Whenever the green light is extinguished, the cause will be displayed until that cause is remedied. This will be displayed on the bottom half of the screen in the format:

Time Condition Location No.

The upper half of the screen will be reserved for CSSMRS/operator communication. Certain messages that appear on the CRT should also be logged on a hard copy printer.

Operator controls should consist of a 10-digit key pad and a group of function keys. The latter include at least the following: Acknowledge, Location Select, Access, Normal, Arm Feds, Disarm Feds, Fire Feds, Confirm, TV on, TV off, Login, Logout. In addition there should be a joy stick and zoom control for CCTV. The CCTV display is separate from the CRT message display. It can be selectively connected to any camera in the CSSMRS installation (multiple CCTV monitors may be desirable).

The "Acknowledge" key must be actuated by the guard to acknowledge the occurrence of an alarm. When this has been done, the other function keys are automatically connected to perform their designated functions at the location indicated by the alarm until such time as they are

associated with another location by use of the "Location Select" key.

The "Location Select" key, together with the ten-digit key pad, permits the guard to select a location to which the other function keys are to be connected.

The "Access", "Normal", "Arm Feds", "Disarm Feds", and "Fire Feds" keys perform those functions at the location which has been selected. The "Arm Feds", "Fire Feds", and "TV on" functions are disabled at a location that is in "Access" mode. The "Confirm" key is used to validate certain commands to minimize the chances of operator error. A command which does not receive a required confirm within 15 seconds is automatically erased; it is also erased if it is replaced by another command.

The "TV on" and "TV off" keys, together with the camera controls, permit the guard to examine the selected location via CCTV except when the location is in "Access" mode.

The "Login" and "Logout" keys permit a record to be maintained of the current guard(s) on duty by using the ten-digit key pad to report their identity.

An illustration of the operations of the controls and displays will help to clarify their functions and use.

Sgt. John Jones arrives at the center for guard duty beginning at 08:00. The green light on the map display is on. He activates the "Login" key followed by the digits 214. His assigned identity number is 215, but he made a mistake in keying. The top half of the CRT display shows the following message:

214 on duty, 08:00

Confirm.

The "confirm" portion of the message is blinking.

Sgt. Jones realizes he has made a mistake so he activates "Login" followed by "215". The message on the CRT is replaced by:

215 on duty, 08:00

Confirm.

"Confirm" is again blinking. Jones activates the "Confirm" key and the screen goes blank. The login is recorded on the printer.

At 08:10 operations personnel arrive and request access to magazine 15. Jones actuates in succession "Select Location" "15" and "Access". The top portion of the display shows the message "Access mode requested, location 15, Confirm." Confirm is again flashing. Jones

presses "Confirm". The message disappears. CSSMRS sends a message directly to the microprocessor at location 15 to set "access" mode. The microprocessor at location 15 does so and confirms the action. CSSMRS sends a message to higher headquarters advising of this action and the lower portion of the display shows the message:

(1) Access Mode Location 15 08:11.

The green light on the map display goes out and an amber light at location 15 comes on. The display message is logged on the printer.

From this time on the CSSMRS processor repeats the access mode command message to the location 15 microprocessor on each polling cycle to verify the continuing authenticity of that command. Failure to receive the polling message within the polling cycle period will cause the microprocessor to revert to "normal" mode.

At 09:00 Jones receives a radio message that operations are complete and they have vacated and locked magazine 15. In actuality, although they have closed and padlocked the magazine door, it was not completely seated and its magnetic switch is still in the open position. Jones actuates "Select Location" "15" and "Normal" in sequence. The CSSMRS processor sends the appropriate message to the location 15 microprocessor which complies and immediately returns a message that an alarm condition exists on the magazine door. CSSMRS deletes the display of message (1) and replaces it with

(2) Door Alarm, Location 15, 09:01

on the lower portion of the display screen and logs it on the printer. This, together with the message "Acknowledge" on the top part of the screen, are blinking. The yellow light at location 15 on the map display is replaced by a flashing red light.

Jones presses "Acknowledge" and the flashing display lamp goes to steady state. The "Acknowledge" message on the top of the screen is replaced by the guidance message "Check area with TV".

The alarm condition has automatically selected location 15 for Jones' controls, so all he has to do is press "TV on". The CSSMRS processor sends the appropriate message to the location 15 microprocessor and light and camera are activated in the magazine. The lower portion of the CRT adds the message

(3) TV on Location 15, 09:02

Using the camera controls, he scans the area verifying that there is no one inside the magazine. He activates "TV off" and message (3) is deleted from the screen. The time that TV was turned on and off is logged on the printer. Jones then activates "Access" and "Confirm", the

latter in response to the blinking request on the display. After the appropriate exchange of messages between the CSSMRS processor and the location 15 microprocessor, the red light on the map display is replaced by amber and the CRT display shows:

(4) "Access mode Location 15, 09:04"

Jones then radios the personnel outside of location 15 to to re-close the door more securely. They comply and this time when Jones activates the "Normal" button the amber light is replaced by the green light on the map display and message (4) is deleted. "Site Secure" messages are logged on the printer and transmitted to higher command.

The top portion of the CRT display now shows the following instructional message to Jones:

"Log disposition of 09:01 Alarm - Acknowledge"

"Acknowledge" is blinking.

Jones makes the appropriate log entries and actuates the "Acknowledge key" and the display is cleared.

At 09:30 the CSSMRS generates and displays the message:

"Suggest a walk test of perimeter segment 24
- Acknowledge"

Jones acknowledges and the display is cleared. He then dispatches a roving patrol to conduct the walk test. At 09:40 an alarm occurs on segment 24. Jones acknowledges the alarm, verifies that it was caused by the patrol which he recalls and then resets the system by actuating the "Normal" key. Then in response to CSSMRS display prompting, he logs the disposition of the alarm as a routine test.

The foregoing description of the CSSMRS is far from complete; it merely provides an overview of the major attribute and characteristics that are considered necessary and desirable for incorporation in any final design configuration. It will be the objective during Phase II to complete the CSSMRS system definition and develop specification that can be used for the procurement of one or more prototypes. The proposed Phase II work plan is contained in section III of this report.

Section III

Phase II Work Plan

The overall objective of the work that will be undertaken in Phase II is to complete and formalize the definition of the CSSMRS and to prepare specifications that could serve as the basis for the procurement of one or more prototype systems for field installation, test, and evaluation. In order to accomplish this, it will be necessary to cover in detail and definitize all of the items on the following outline. This will require the selection of alternatives and the resolution of questions such as those which were discussed in Section II of this report. In some of these cases it is believed that laboratory tests and experiments may be necessary in order to develop data that will support and justify rational decisions. In other instances, further study, analysis or consultation may provide an adequate basis for a design choice.

I. Remote Microprocessor

A. Functional characteristics - speed, power, types and amount of memory, environmental tolerances, power requirements.

B. Interface Requirements -

1. Inputs - numbers and types of sensors, numbers and types of tamper alarms, status signals from safe/arm mechanisms and standby power source, digital data link.

2. Outputs - CCTV camera controls, pan/tilt/zoom, lights, local audible alarm, actuation of sensor test stimuli, safe/arm and actuation of FEDS (numbers and types), reset of override decoder.

C. Location - housing and tamper alarm arrangements at the magazines and on the perimeter of the site.

D. Software - development of flow charts.

1. System

2. Applications

3. Diagnostics

E. Documentation - establish requirements.

1. Hardware

2. Software

II. Data Communications Link (On Site)

A. Use of fiber optics, coaxial cable or both.

1. Further cost and performance analysis required.

2. Configuration - repeaters, power dividers.

B. Video Data

1. Number of channels and bandwidth required.

2. Method of multiplexing with other channels and with digital data, TDM, FDM, or separate channels.

C. Digital Data

1. Data rates - inbound, outbound.

2. Communications control protocols - polling interval, contention considerations.

3. Security and integrity - use of crypto or line sypervision.

D. Documentation Requirements

III. Forced Entry Deterrent Systems (FEDS)

A. Activation or firing circuit requirements.

B. Safe/arm units - electronic, key operated manual.

C. Safe/arm override - key, decoder, timer, connector, status display, reset.

D. Documentation requirements.

IV. Central Processor

A. Functional characteristics - speed, word size type and amount of memory, environmental tolerances, power requirements (uninterruptable).

B. Redundancy - spare processor for backup or two processors always on, possibly one running basic application programs and the second collecting environmental background data for nuisance alarm correlation.

C. Housing - location, security and protection of processor and peripherals including memory, power and I/O connections.

D. Interface requirements.

1. Inputs - numbers and types of sensors or signal sources.

(a) Environmental
(b) Duress
(c) Guard activity
(d) Personal identity verification
(e) Word recognition
(f) Trace material detectors (FEDS)
(g) Digital data links
(h) Operator commands

2. Outputs

(a) Digital data links
(b) Operator displays
(c) Speech synthesis
(d) logging printer

3. Automatic switchover arrangements with redundant processor.

E. Software - development of flow charts.

1. Operating system

2. Application programs

(a) Development of programmed repertory of tactics in response to sensed intrusion/attack situations. (This requires support from user service tacticians.)

3. Diagnostics

F. Documentation - establish requirements.

1. Hardware

2. Software

V. Controls and Displays

A. Site overall status display - map board or CRT, size modularity, features.

1. Microprocessor status display driver(s) - hardware, software.

B. Operator's message display unit

1. Ten-digit key pad

2. Function keys - system commands

3. Logging printer

C. CCTV monitors - number, size.

1. Pan/tilt/zoom controls

D. Audible signals

1. Alarms

2. Voice answer back - synthesized.

E. Documentation - establish requirements.

VI. Data Link to Higher Headquarters

A. Need for multiple routing and NSA handling.

1. Land line, microwave, satellite.

B. Content and criteria for traffic.

Throughout the process of definitizing these items, it is imperative that a highly reliable system must be the final result. Special attention must be given to software reliability to insure that computer programs function in the intended manner and do not lead to anomalous or erroneous results. This will involve extensive testing and validation and may necessitate the development of new techniques to authenticate the quality, integrity and reliability of software to insure that all design objectives are met.

The developmental time frame of some of the CSSMRS components is expected to span a considerable period of time. For example, it is expected that some of the FEDS may become available for testing much sooner than will the trace materials for incorporation in them, and that the trace material detection equipment and techniques may be even further in the future. Word recognition equipment of limited capabilities is available now, but improvements in performance are being made at a rapid rate.

These considerations suggest that the specifications for the CSSMRS should be developed in a form which would support an initial "core" capability that could be readily expanded to accept additional desired system components and capabilities as these become available. This modularity of approach has been reflected in the evolving CSSMRS concepts described in Section II of this report and in the work plan outlined above. It will continue to be a major factor as future work progresses.

BS-114A (REV. 7-73)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO. NBSIR 77-1262	2. Gov't Accession No.	3. Recipient's Accession No.

TITLE AND SUBTITLE

COMPUTERIZED SITE SECURITY MONITOR AND RESPONSE SYSTEM

5. Publication Date: June 1, 1977

6. Performing Organization Code: 650.01

AUTHOR(S): R. T. Moore; R. J. Carpenter; A. L. Koenig

PERFORMING ORGANIZATION NAME AND ADDRESS

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20234

8. Performing Organ. Report No.

10. Project/Task/Work Unit No.: Project 6509410

11. Contract/Grant No.: DNA IACRO 77-805

. Sponsoring Organization Name and Complete Address (*Street, City, State, ZIP*)

Defense Nuclear Agency
Washington, D. C. 20305

13. Type of Report & Period Covered: Report to Sponsor

14. Sponsoring Agency Code

. SUPPLEMENTARY NOTES

. ABSTRACT (*A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.*)

'he Computerized Site Security Monitor and Response System (CSSMRS) was conceived as n integrated, state-of-the-art, computer-based system to enhance and improve the verall physical security of storage sites for special weapons or materials.

'his report is divided into three sections. Section I contains an overview summary of he findings or study results for each of the eight specific Phase I tasks. These are et forth in varying degrees of detail as appropriate to both the nature of the task nd the results.

ection II is a description of the CSSMRS in its current (and incomplete) state of volution. Here many of the attributes, capabilities, and features developed during he course of Phase I work are set forth. Some of the alternatives are identified as re areas where additional work will be necessary to reach clearly identifiable and ttainable objectives necessary to complete the system definition.

n Section III, a proposed Phase II work plan is presented.

KEY WORDS (*six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons*)

dversary scenarios; automated response systems; distributed processing; onitoring systems; physical security; sensor systems.

AVAILABILITY

[X] Unlimited

[ ] For Official Distribution. Do Not Release to NTIS

[ ] Order From Sup. of Doc., U.S. Government Printing Office Washington, D.C. 20402, SD Cat. No. C13

[X] Order From National Technical Information Service (NTIS) Springfield, Virginia 22151

19. SECURITY CLASS (THIS REPORT)	21. NO. OF PAGES
UNCLASSIFIED	44
20. SECURITY CLASS (THIS PAGE)	22. Price
UNCLASSIFIED	$4.00