96th Congress
2d Session

COMMITTEE PRINT

RECENT FALSE ALERTS FROM THE NATION'S MISSILE ATTACK WARNING SYSTEM

REPORT

OF

SENATOR GARY HART

AND

SENATOR BARRY GOLDWATER

TO THE

COMMITTEE ON ARMED SERVICES

UNITED STATES SENATE

OCTOBER 9, 1980

Printed for the use of the Committee on Armed Services

U.S. GOVERNMENT PRINTING OFFICE
68-531 O WASHINGTON: 1980

REPORT ON RECENT FALSE ALERTS FROM THE NATION'S MISSILE ATTACK WARNING SYSTEM

On June 20, 1980, the Chairman of the Senate Armed Services Committee, Senator John C. Stennis, asked Senators Gary Hart and Barry Goldwater to investigate recent false alerts in the Nation's missile attack warning system. This report is the result of that investigation and concentrates on the false alert incidents of June 3 and June 6, 1980. In making this investigation, Senator Hart visited the National Military Command Center at the Pentagon and the North American Aerospace Defense Command Center in Colorado Springs, Colorado where he was briefed on the cause of the incidents and steps taken to prevent further occurrences. In addition, staff members of the Armed Services Committee visited Strategic Air Command Headquarters, Offutt Air Force Base, Nebraska. Staff members also held discussions with a number of responsible officials from the Office of the Secretary of Defense; the Organization of the Joint Chiefs of Staff; and Headquarters, United States Air Force.

This report covers the following subjects:

(1) a description of the missile attack warning system;
(2) a description of the events of June 3 and June 6, 1980;
(3) descriptions of the cause of the incidents and steps taken to reduce the possibility of recurrence;
(4) discussion of the significance of these incidents;
(5) a critical analysis of the organizational and command relationships of the missile warning function; and
(6) a critical analysis of the procedures for procurement of automatic data processing equipment for the missile warning system.

MISSILE ATTACK WARNING SYSTEM

The Missile Attack Warning System consists of three major segments (1) sensors to detect missile launch, (2) computer centers and communication links to analyze and distribute the data from the warning sensors, and (3) command posts where the implications of the warning information are assessed and appropriate actions directed. Major components of each segment are as follows:

MISSILE WARNING SENSORS

—Infrared warning satellites
—Ballistic Missile Early Warning System (BMEWS)
—PAVE PAWS, a phased array radar for detecting submarine-launched ballistic missiles (SLBMs)
—Perimeter Acquisition Radar Attack Characterization System (PARCS)

—Two radars in the southern United States for detecting SLBM launches
—Cobra DANE radar at Shemya, Alaska

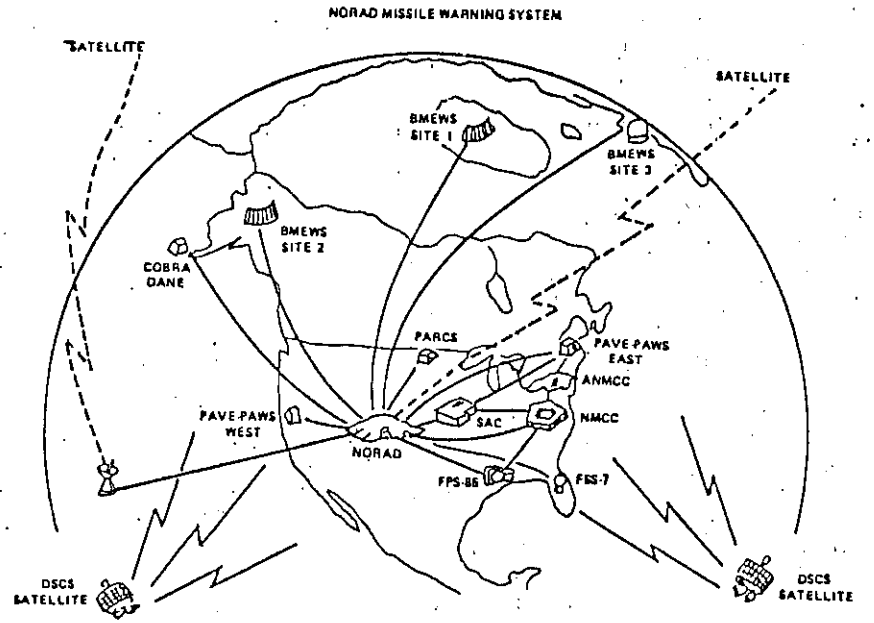
COMPUTER COMPLEXES AND COMMUNICATION LINKS

—Ground stations in the Continental United States and overseas
—Other computer processing stations colocated with the sensors

COMMAND POSTS

—North American Aerospace Defense Command (NORAD)
—Strategic Air Command (SAC)
—National Military Command Center (NMCC) (Pentagon)
—Alternate National Military Command Center (ANMCC (Fort Ritchie, Maryland)

Figure 1, taken from the GAO report "Review of Department of Defense's Strategic Missile Warning System", March 14, 1980, depicts the schematic arrangement of the NORAD missile warning system.



The missile warning system employs a two-step process for identifying a missile launch and assessing the threat to the North American continent. First the infrared warning satellites detect the infrared signature of the burning missile motor.

Ground-based radars provide a second source of data which relies on detection of a different physical phenomenon, i.e., radar tracking of a physical object as opposed to detecting the infrared signature

of a burning missile motor. The BMEWS radars would be the first to detect Soviet intercontinental ballistic missiles (ICBMs); the Pave Paws would be the first to detect SLBMs launched off the east or west coasts. Two older radars located in Florida perform the same function for missiles coming from the Gulf of Mexico.

The dual phenomenology detection system has been a fundamental and critical design feature of our missile warning system for many years and provides an important cross-check for evaluating ambiguous data.

If the Soviets were to launch SLBMs and ICBMs separately or simultaneously, the following sequence of events would most likely take place. The first indication of missile launch would come from the satellites, followed next my Pave Paws detection of SLBMs, and several minutes later BMEWS detection of ICBMs.

—The satellites should detect launch of both the SLBMs and ICBSs shortly after launch.
—The Pave Paws radar should pick up the SLBMs within minutes after launch.
—The BMENWS should pick up the ICBMs several minutes later.
—The PARCS should pick up the ICBMs in their terminal phase of flight.

The time between launch and impact of SLBMs could be short and less than that of the ICBMs. The time between launch and impact of ICBMs would be about 30 minutes. Since SLBMs could destroy a large part of our ground-based sensors and command posts, it must be assumed that the time from detection to the first impact during which we will have full use of our present system could be short. This does not mean that the entire system would disappear at the end of this period, but that we would become dependent on those assets that could survive the initial attack, in general those which become airborne in time to escape the attack. So there is high premium on the full and effective utilization of the short period between detection of attack and destruction of a major part of the command and control infrastructure.

The satellites and the Pave Paws radar, the two sensors that are designed to detect attack of SLBMs, feed their data directly to all four major command posts (NORAD, SAC, MMCC, and ANMCC) so that all four are looking at the data received directly from the sensors and are evaluating it simultaneously. NORAD also transmits to the other three command posts it analysis of SLBM attack data so that duty officers at the three command posts (SAC, NMCC and ANMCC) have two separate computations and displays of SLBM attack data, one coming directly from the sensors and the other from NORAD. Data from all other warning sensors are fed only to the NORAD command post where it is analyzed with the results transmitted to the three other major command posts.

In order to insure that the communication lines between NORAD and the three other command posts remain open, NORAD constantly transmits messages to the three command posts over the circuits that would be used to transmit the message of an actual attack. Normally the message is just a filler so that all three command posts can monitor the condition of their communication links from NORAD. If the system is working properly, all four command posts have the same data

available to them. When there is any indication of a real threat or even ambiguous data, the four command posts begin a formal conferencing procedure to evaluate and assess the data. Three types of formal conference are used:

—Missile Display Conference.
—Threat Assessment Conference.
—Missile Attack Conference.

Missile Display Conferences

The satellites trigger the warning process by observing the infrared signatures of the missiles and comparing them with previously observed infrared signatures from Soviet missiles. Unfortunately, there are other physical phenomena both in the atmosphere and on the Earth's surface which can give similar infrared indications. The detection system must be sensitive enough so as to not miss any missile launches, but still not overburden the system with irrelevant information. Achieving this balance is a continuing problem. As a result of the need to maintain a sensitive system, there are many indications of detections that have to be evaluated but prove not to be associated with a threatening missile launch. In addition there are routine missile display conferences called when changes are made in the positioning or configuration of the sensors that might cause the system to yield unusual information. In 1979 there were 1,544 routine missile display conferences that were necessary to deal with events other than threatening or ambiguous missile launches. There were 78 missile display conferences called to evaluate detections that were possibly threatening to the North American continent. In 1980 through June 30 there were 2,159 routine missile display conferences and 69 called to evaluate possible threats to North America.

All 3,703 of the routine missile display conferences held in 1979 and through June 30, 1980 resulted from actual pickup by warning sensors of some physical phenomenon or reconfiguration of warning sensors. In addition to these incidents there is the possibility that a computer or a piece of communications equipment will transmit a false piece of information. This happens with some frequency although prior to the June 3 and June 6 incidents records were not kept of actual incidents. NORAD spokesmen indicated it may happen two or three times a year. These incidents result from random failures within the computer and communications hardware and software and not as the result of external stimuli.

So there are several sources of false indications of warning that are possible, including the actual detection of an infrared signature which must be evaluated because it bears close enough resemblance to an ICBM or SLBM signature so that it cannot be ignored and the random malfunction of a piece of computer and communications equipment. The missile warning system handles on a daily basis the problem of sorting out false indications of attack from potential real indications of attack. The missile display conference, the first step in evaluating sensor data, is terminated when the Commander-in-Chief (CINC) of NORAD makes the judgment that all the available data indicate either the presence or absence of a threat to North America.

Threat Assessment Conference

If the NORAD Commander determines the possibility of a threat, the next step is to convene a threat assessment conference. This brings more senior people than the duty officers at the various command posts into the evaluation, such as the Chairman of the Joint Chiefs of Staff. A threat assessment conference is convened to determine the nature of the threat to North America and to direct preliminary steps to enhance force survivability. In 1979 and 1980 there were four threat assessment conferences. They were called on the following occasions and for the following reasons:

October 3, 1979.—An SLBM radar (Mt. Hebo) picked up a low orbit rocket body that was close to decay and generated a false launch and impact report.

November 9, 1979.—False indications of a mass raid caused by inadvertent introduction of simulated data into the NORAD Computer System.

March 15, 1980.—Four SS–N–6 SLBMs were launched from the Kuril Islands as part of Soviet troop training. One of the launches generated an unusual threat fan.

June 3, 1980.—False indications caused by a bad chip in a communications processor computer.

Missile Attack Conference

If the threat persists, the final action taken is to convene a missile attack conference which brings in all senior personnel including the President. No such conference has ever been convened.

EVENTS OF JUNE 3, 1980

On June 3, 1980 at approximately 2:26 a.m. Eastern Daylight Time, the SAC command post display system indicated that two SLBMs had been launched toward the United States. Eighteen seconds later, the display system showed an increased number of SLBM launches. SAC command post personnel called NORAD command post personnel regarding this display and the NORAD personnel stated they had no indication of any launched SLBMs. Shortly after the initial indication, the SAC duty controller directed all alert crews to move to the alert aircraft and start their engines in order to prepare to take off should that become necessary in order to survive. After a brief period, the SAC display cleared, showing no threatening SLBMs; NORAD reported no indications of SLBMs were coming from the sensors (satellites or radar); and no data were being transmitted to the SAC, NMCC or ANMCC command posts. Shortly thereafter, the SAC aircraft crews were directed to shut down their engines but to remain in their aircraft.

NORAD reported all systems clear. After a brief period, the warning display at SAC indicated that Soviet ICBMs had been launched toward the United States. After another interval, the NMCC command post received indications that SLBMs were launched toward the United States.

All of the indications of threatening missiles received at the SAC command post and the NMCC command post were on the circuit that

receives data from the NORAD command post, not directly from the sensors themselves. The NMCC Duty Officer convened a missile display conference to evaluate the situation. This conference continued while the four command posts tried to determine the source of the data. All command posts were convinced the data were erroneous and invalid.

The NMCC Duty Officer convened a threat assessment conference as a way of terminating the incident and insuring that all parties knew that there were no threatening activities. As part of the normal activities associated with a threat assessment conference, the airborne command post of the Pacific Command prepared for takeoff as a survivability measure. After a brief period, the Commander of NORAD confirmed there was no threat. But as part of the ongoing reaction of the threat assessment conference, the Pacific Command airborne command post took off after this. The NMCC Duty Officer terminated the threat assessment conference. One minute later SAC terminated its alert and the alert crews returned to their barracks.

Interviews with Air Force personnel indicate that within minutes of receiving a first indication of threatening missiles all of the command posts concluded the data were erroneous. They reached these conclusions based on three observations: (1) there was no indication from the sensors of any detection of missiles; (2) the indication on the display that was being received from NORAD did not follow any logical pattern or sequence of events that would be expected from a missile launch; and (3) the different command posts were receiving significantly different indications. The data appeared to be random in nature because of the changes in both the number of missiles and the patterns of display at the SAC command post and the NMCC command post.

Even though the command post controller prevented any undue reaction to the false and erroneous data, there seemed to be an air of confusion following the determination that the data were erroneous. This raises the question that when compared with data or scenarios that are different from what would be the most likely scenario, can the procedures and trained personnel deal with an unusual situation in such a way that they do not negate the effectiveness of the entire system while they are searching for the cause or source of stray or erroneous data. In other words, while the controllers at the various command posts were quite effective in recognizing and dealing with erroneous data, could they have dealt with a real attack if it were preceded by stray and erroneous data introduced into the system?

This question raises the issue of the effectiveness and usefulness of checklists and training for command post personnel. Clearly, in the event of a real attack, checklist would be very useful since the pressure and tension would be very high and it would be mandatory that well thought-out procedures developed in advance be available for the use of the controllers and other senior officers. On the other hand, is it possible to develop checklists to cover every possible scenario and is the training given to the controllers adequate to give them a balance between reliance on checklist and application of sound judgment?

EVENTS OF JUNE 6, 1980

Following the June 3 incident NORAD took a number of steps to determine the source of the error and to isolate the offending piece of equipment. In order to do this, NORAD tried to duplicate the error by running its system in the same configuration as was being used on June 3 hoping to reproduce the erroneous data so as to be able to isolate its source. On June 6, at 3:38 p.m., the mistake was reproduced with SAC again receiving indications of attack by ICBMs and the NMCC receiving indications of threatening ICBMs. Again there was no indication of such attack on the displays coming from the sensors but only on the display coming from the processed data from NORAD. Again, the SAC alert crews were sent to the alert aircraft to start engines in preparation for takeoff should that become necessary in order to survive. This occurred shortly after the initial data were received. Subsequently, the SAC crews were directed to shut down their engines but to remain in their aircraft. Within minutes the data were assessed to be false and NORAD reported its assessment that there was no threat.

However, the incident continued as more indications of missiles launches were received at SAC and NMCC as efforts continued to determine the source of the error. At the completion of the June 6 incident, NORAD switched its computers to what is known as the mission essential backup unit, a standby computer in case the main system failed.

CAUSE OF THE JUNE 3 AND 6 INCIDENTS

Following these two incidents NORAD and DOD made an intensive sffort to locate the source of the erroneous data and to correct it. In doing this they used personnel of NORAD as well as computer and communications experts available from government and industry. The conclusion of these investigations was that the failure was caused by a faulty integrated circuit in a communications multiplexer. The communications multiplexer is not part of the data analysis computer, but is part of the communications system which takes the results of the analysis and puts it into message form for transmission to the other command posts. The multiplexer forms the message which NORAD transmits continuously to all command posts plus to the Canadian Headquarters in Ottawa in order to have a continuous check on the condition of the circuits. Normally in that part of the message which indicates how many SLBMs or ICBMs have been launched, the display will indicate zeros. The effect of the failure of this particular integrated circuit was to fill some of those zeros with the number 2 and to do it on a random basis both as to which command post received the data and to which fields of data had the 2's in them.

STEPS TAKEN TO REDUCE THE POSSIBILITY OF RECURRENCE

NORAD has employed computer and communications specialists from both government and industry to develop a series of corrections to minimize the possibility of these types of incidents. A listing of

the actions completed or in progress is contained in Appendix A. However, some of the more significant ones are:

—First, NORAD has added computer porgrams that have the effect of tracing a message through the entire message preparation phase to insure that the transmission accurately reflects that which is input through the message system.

—Second, they have added a display in the NORAD command post which will show what is being transmitted to the other command posts. Prior to this, NORAD had no way of knowing what was being transmitted to other command posts.

—Third, the message being transmitted from NORAD to the other command posts has been changed in format. Formerly the message was of the same format that would be used in case of an actual attack, but the space where the numbers of missiles in the attack would be shown was filled with zeros. Now, that message is in a different format which just indicates the status of the communications system rather than any indication of numbers of missiles. Should the communications system at NORAD transmit a message giving numbers of attacking missiles, an alert in the NORAD command post would be triggered indicating a transmission of a real message.

—Fourth, another interim change has been made at SAC where the duty officer was instructed to alert the bomber and tanker ground force upon any indication of misisle attack. Now, under most conditions, he is instructed to compare warning data being received directly from the warning systems with that being received from NORAD.

SIGNIFICANCE OF THE JUNE 3 AND 6 INCIDENTS

The June 3 and 6 incidents illustrate that the missile tactical warning and threat assessment task is a very complex and difficult technical task which will produce some ambiguities and uncertainties. To accomplish it we rely on a combination of satellites and ground-based radars located around the world coupled with computers and communications systems to bring this data together, analyze it and transmit it to those who need it in a very short period. We could not do this task without computers and high-speed communications systems. It is not surprising that such a complex and challenging task produces some erroneous data. But even though we are dependent on computers and high-speed communications, we are not controlled by them. At every step of the process, experienced trained personnel evaluate and make judgments on the meaning of the data and only these personnel can direct any action in response to what the warning system tells us.

In no way can it be said that the United States was close to unleashing nuclear war as a result of the June 3 and 6 incidents. In a real sense the total system worked properly in that even though the mechanical electronic part produced erroneous information, the human part correctly evaluated it and prevented any irrevocable reaction.

The fact that SAC dispatched all the alert crews to the bombers and tankers was not an untoward move. It was a prudent step to enhance the survivability of the bombers and tankers should this country be under attack. It is quite appropriate and necessary that this step be taken very early to prevent any possible threat because there are very few minutes available for the aircraft to escape a threat. The fact that these steps are taken to enhance survivability of the aircraft does not lead automatically to their dispatch on the nuclear attack missions. There are many more steps, all controlled and executed by senior civilian and military leadership, that must be taken in order to dispatch on nuclear attack missions. The Commander of SAC must have the authority to take these modest steps to enhance the survivability of the bomber and tanker force.

ORGANIZATIONAL AND COMMAND RELATIONSHIPS FOR THE MISSILE WARNING FUNCTION

One of the more disturbing conditions found in the investigation is the organizational and command relationships of the missile warning function. We found no evidence that these relationships contributed in any way to the incidents of June 3 and 6, but they are cause for concern in the long run because they do appear to be detrimental to good management. In the reorganization of the Aerospace Defense Command (ADCOM), the responsibilities for the management and the maintenance and operation of all early warning sensors were transferred to SAC and the communications-electronics systems to Air Force Communications Command (AFCC). (ADCOM is a specified U.S. command that has responsibility for air and space defense of the United States. The U.S. portion of NORAD, which is a United States-Canadian command, is part of ADCOM). All that remains at ADCOM is the management and operation of the command post at Cheyenne Mountain and responsibility for the interpretation of the data made available to them in Cheyenne Mountain by SAC and AFCC resources operating under the operational control of CINCAD COM who is also CINCNORAD.

In effect, the responsibility for the management of the missile warning assets is divided among three major commands within the Air Force with a fourth, the Air Force Systems Command (AFSC), being responsible for the development of new equipment for missile warning functions. The reason for this unusual arrangement seems to be found in the history of the past 10 years of the air defense mission. The air defense forces of this country have been drastically reduced over the past 10 years and the responsibility for the management and operation of them transferred to the Tactical Air Command. As this reduction was taking place there was increasing pressure, much of it congressional, to reduce the size of ADCOM and its management headquarters. Coincidentally, the missile warning function, also the responsibility of ADCOM, has been fragmented and spread out among the Air Force as part of this effort to reduce management headquarters at ADCOM. What appears to have happened is that the decreasing air defense mission with its resultant lack of priority in assignment of resources has carried over to the missile warning function. This appears to be very unfortunate because the missile warning mission requirement has not decreased in scope, importance or criticality; in fact, it has increased. It is difficult to understand how resource management has been allowed to be splintered and fractionated among three commands

of the Air Force while operational control remains assigned to the specific command—ADCOM.

In our investigation and discussions with military officers and civilians throughout DOD there seems to be agreement that the total missile warning function should be consolidated under one commander who has the status and rank to insure this mission area is adequately funded and managed. The two most obvious places are to place it in SAC or in the Air Defense Center (ADC). We questioned a number of people as to the wisdom of combining the missile warning and asessment mission with the strategic nuclear response function. In other words, what is the value of having a completely independent assessment of the nature of the attack and then an independent management of the appropriate responses. Although there has been little or no formal study of this question, we found no disagreement with the idea that these two should be separate since both would occur at a time of incredible tension and pressure and involve different considerations and evaluations. Therefore, this appears to be an urgent question that needs more study and thought to determine if the intuitive conclusion is the correct one.

The Air Force has convened a senior panel to review the adequacy of the support and organization of the missile warning function. The panel is led by Lieutenant General Howard Leaf, the Air Force Inspector General, and includes senior officers from SAC, ADC, AFCC, AFSC, and Headquarters, United States Air Force. It is anticipated that their report will be completed during the Fall of 1980. It is not clear that this panel will make recommendations regarding overall organization of the missile warning function.

PROCUREMENT OF AUTOMATIC DATA PROCESSING EQUIPMENT FOR THE MISSILE WARNING MISSION

Another aspect of the management of the missile warning mission that is cause for concern is the existing procedure for acquiring automatic data processing (ADP) equipment.

The ADP acquisition process is a highly regulated and complex system. This is the result of extensive fragmentation among Federal agencies of responsibilities for ADP approvals, classification, funding, standards, and acquisition policy.

Public Law 89–306 was enacted October 30, 1965, "to provide for economic and efficient purchase, lease, maintenance, operation, and utilization of automatic data processing equipment by Federal departments and agencies". The House Committee on Government Operations actively oversees the Federal Government's ADP resource acquisition practices. Public Law 89–306 assigns the following responsibilities:

—To the agencies (DOD is an agency)—The responsibility to approve requirements.

—To Office of Management and Budget (OMB)—Fiscal and policy control for implementation of the law.

—To General Services Administration (GSA)—Sole procurement authority.

The key to understanding the ADP acquisition process in view of the Public Law 89–306 is to recognize that it established three levels of approval which must be obtained prior to any ADP resource acquisition.

Requirement Approval.—The agencies are solely responsible for determination and validation of their ADP requirements. The Military Services have established various processes for validation and approval of ADP requirements.

Budget Approval.—OMB has responsibility for approval of agency-identified budget requirements. This is accomplished through the normal DOD Planning, Programming and Budgeting System (PPBS).

Procurement Approval.—GSA has the responsibility for procurement approval. This is normally accomplished by a Delegation of Procurement Authority (DPA) to the agency. GSA has established Federal Procurement Regulations (FPR) and Federal Property Management Regulations (FPMR) that uniquely pertain to ADP resource acquisitions. These regulations are in addition to the Defense Acquisition Regulations (DAR) which normally govern DOD procurements.

The basic elements of an ADP acquisition—requirements approval, delegation of procurement authority and acquisition are governed by a series of regulations which were derived through the implementation of the Public Law 89–306. The requirements approval process is governed by those agency regulations which address the requirements validation process. In the Air Force the 300-series regulations were developed specifically to address management and acquisition of ADP resources. Typically the requirements approval process takes approximately six to nine months for an ADP acquisition.

Following the requirements approval process for those acquisitions exceeding agency thresholds, a delegation of procurement authority is required from GSA. This is normally accomplished within a six to nine-month period. This process has become more extended as the GSA has required more information relating to the requirements validation process than in the past. Two recent changes in regulations will have significant impact on the length of time required for this process. The first concerns the requirement for a "feasibility study" for each approved requirement for ADP resources. In most cases, systems are already automated and the feasibility for automating a process has been proven, thus, the need to determine feasibility becomes a superfluous task. The second change concerns the development of a "software conversion study" for new or modified ADP systems. This requirement only makes sense when there is a significant amount of direct computer program code which must be translated/converted in conjunction with the ADP acquisition. In most cases where new development is required and the selected alternative defines a new architecture or an upgrade within a given computer manufacturer's line, the need for a software conversion study is not appropriate and only presents yet another roadlock in the process of ADP acquisition. The software conversion study requirement has been so structured that all new requirements must allow additional processing time to accommodate this effort even thought it may not be applicable to the task identified. The potential impact of these new changes in GSA requirements could add up to a year to the requirements approval process, thus further extending the time line for ADP acquisition.

Once a delegation of procurement authority is received by an agency, the acquisition/procurement process can begin. Depending on the complexity of the acquisition, this phase can take from one to five years before an operational capability can be achieved.

Acquisition of command and control systems within the DOD has been particularly encumbered by the application of the established regulations for Federal ADP acquisition. In the particular area of strategic and tactical warning, a typical system upgrade or improvement consumes five to seven years from concept definition to operational capability. During this extensive validation, development, and procurement period, the operational concepts for use of the system often change as new weapon systems are introduced into the command control structure. In most cases, the ADP equipment is functionally obsolete prior to its operational use.

This acquisition cycle can only be reduced when an urgent need has been established at the DOD level. An example of this urgency was recently demonstrated in the processing and subsequent acquisition of the NORAD Off-Site Test Facility (OSTF). The need was recognized at a high enough level and expeditious action was taken to minimize the impact of the complex regulatory structure. The requirement approval and procurement approval processes, which would normally have taken 12–18 months, were accomplished in less than two months. An operational capability will be attained in less than one year.

The normal acquisition process to support command and control requirements should be as responsive as the OSTF acquisition. In this way, command and control systems could maintain the required functional currency to meet the demands of the operational environment. In order for NORAD to upgrade or replace an element within its command and control system, an inordinate amount of time is required under the current process. The current operational system was conceived in 1968 and was brought on line in 1979. A process needs to be established to incrementally replace selected functional elements in a responsive manner. Current plans are to upgrade and replace these functional ADP elements over the next eight years. However, under the current regulatory process, the planned period of time for system upgrade could more than double.

This dilemma could be resolved if a blanket delegation of procurement authority were granted to the Department of Defense for ADP acquisition for those critical command and control systems, such as the NORAD system which provides the primary strategic and tactical warning systems for the United States. A precedent has been established in other government agencies, such as the National Aeronautics and Space Administration, National Security Agency, Defense Intelligence Agency, and Federal Bureau of Investigation, for blanket delegations to allow more flexibility and responsiveness to meet agency mission needs. The result of such an action for the critical command and control systems within the DOD would significantly reduce the required acquisition time for ADP systems.

CONCLUSION AND RECOMMENDATION

The missile attack warning system is an extremely critical part of the defense structure of this country. It is a highly technical and complex system spread around the world and into outer space. It is a system which must be prepared to deal with uncertainties because they will occur whether caused by physical phenomena similar to launch of missiles, misinterpretation of actual detection of missile launch, or simple failure within the vast array of computers and communication equipment which are necessary to make the system operate. The men and women who operate the system recognize the need to deal with uncertainties.

The Department of Defense has taken what appear to be appropriate steps to examine the technical aspects of the system to try to reduce the room for error in handling these uncertainties. There is no guarantee that false alerts will not happen in the future. They will occur and we must rely on the collective judgment of the people manning the system to recognize and deal correctly with false alarms. Both the Office of the Secretary of Defense and Headquarters, United States Air Force are reviewing the procedures and the support provided to the missile warning function. It is recommended that upon completion, the Air Force report be forwarded to the Armed Services Committees of the House and Senate for review.

Two major areas of the missile warning function need to be more carefully analyzed and considered than is being done in the short-term review of the technical qualifications of the system and the procedures for operation of the system. First is the organization of the management of the missile warning function. Since the system's management is divided among four major commands within the Air Force, it is difficult to conclude that it is treated as a true overall system. The organizational structure now existing works to fragment management responsibility and to complicate the process of insuring a highly integrated and smooth working process; however, it is noted that operational control is exercised by CINCNORAD alone.

It is recommended that the Secretary of Defense study this mission area with the objective of consolidating essential resource management under one commander. However, our investigation leads to the conclusion that we should continue to keep separate the operational responsibility for determining if the Nation is under attack and assessing the nature of the attack from the responsibility of responding to an attack. It is recommended that the Secretary of Defense provide a report to the Armed Services Committee by March 1, 1981 so that this issue can be further explored during the authorization hearings next year.

The second major concern is the process for acquiring automatic data processing for the missile attack warning command and control function. Procedures now being used for maintaining a system in the best possible technical capability are the same procedures for acquiring computers for processing the payroll and leave records of military personnel. As a result, delays and technical obsolescence are guaranteed in updating and modernization of the system. The missile warning function is too important to be left to these cumbersome procedures. In addition these procedures have the effect of forcing the procurement of the least common denominator in capability rather than the best available. Again the missile warning function is so special and so important that technical capability, not least cost, should be the determining function. It is recommended that action be taken to

exempt acquisition of automatic data processing equipment for the missile attack warning mission from the normal procedures now used by GSA.

It may be that the procedures for updating and modernizing all of our command and control equipment that is used in the actual employment of forces is being seriously affected in a negative way by the procedures being used to procure automatic data processing equipment. Our investigation was not extensive enough to document that fact, but we may have touched just the tip of the iceberg. It is recommended that the Armed Services Committee explore this issue in depth as it affects the military capability of our forces.

APPENDIX A

Following is a list of completed and in-progress analyses to verify the 427M system.

ENGINEERING ACTIONS COMPLETED

(1) Honeywell Information System performed an audit of all Honeywell equipment installed in 427M to verify correct configurations.

(2) Air Force Communications Command performed an extensive wire audit of over 400 circuits comprising over 3,000 wires and corrected wiring errors and documentation errors.

(3) Bolt, Beranek, and Newman (BBN) completed a consultant effort in the design and verification of the implementation of a cyclic redundancy check for the 427M system.

(4) Texas Instruments completed a tarnish analysis of the suspected intermittent chip and concluded that tarnish of the chip was not a contributing factor to the malfunction.

(5) Hauser Labs, Boulder, Colorado completed an analysis of the circuit board, chip and socket to determine if tarnish was a factor in the intermittent failure. Their conclusion was that tarnish was not a factor.

(6) Ford Aerospace and Communications Corporations (FACC), assisted by NORAD systems engineers, completed an analysis of the June failures and performed an analysis of silver tarnish found on the pins of the suspected chip. Conclusions were that tarnish was not a factor and that the 74175 chip was the cause of the June events.

(7) Southeastern Center for Electrical Engineer Educators, after a thorough analysis of the semi-automatic technical control function of the Common System Segment (CSS), completed specific fix actions for 5 and 12 volt power supplies, to include rewiring of the power distribution system, resetting automatic measurement levels and software fixes to the technical control function.

(8) Air Force Academy Chemical Labs completed an analysis of the chip to determine if the tarnish found on the pins of the suspected chip was the cause of the malfunction. Their conclusion was that the tarnish was not a contributing factor.

IN PROGRESS ANALYSES

(1) MIT/Lincoln Labs is currently performing a detailed analysis of the 427M Missile Warning man-machine interface vulnerabilities and procedures.

(2) Teledyne Brown Engineering is currently performing a software audit of module interfaces in the CSS, NORAD Computer System (NCS), and Mission Essential Backup Unit (MEBU). Preliminary findings are:

(a) Good requirements traceability to test plans, procedures and reports exists at the segment level, especially the NCS.

(b) Test verification matrices exist at the segment level.
(c) Octal patches are kept to an absolute minimum and are very tightly controlled.
(d) Test control/safety procedures appear excellent.
(e) NCS has excellent set of support software tools.
(f) Version releases are sized for manageability.

Following is a summary list of projects designed to improve the NORAD 427M capability to provide reliable Tactical Warning and Attack Assessment.

SOFTWARE

(1) *Parity and Cyclic Redundancy Check (CRC).*—Provided powerful extension of end-to-end communications validity checking. National telecommunications expertise was used in development. Complete.

(2) *Status message and format.*—An investigation is underway with the Communication Central Procesing and Display System (CCPDS) community (JCS, SAC, National Military Command Center) to restructure missile warning messages.

(3) *NCS1/NCS2.*—Currently coding a scheme to cause a software switchover in the event of a failure from the Primary NCS to the Secondary NCS for 100 percent backup of missile warning processing. Estimated completion—June 1981.

HARDWARE

(1) *Data Monitors.*—Have been placed on critical Missile Warning Display System (MWDS) lines to alarm operations personnel whenever an active missile warning message is sent. Complete.

(2) *CSS Upgrade.*—Replace the Honeywell 6050 message processors with H6060 computers. This project is approved and funded for June 1981 completion.

(3) *Digital Television Element (DTVE) By-Pass.*—Develop a by-pass to the unreliable DTVE system. Approved but not yet funded for March 1981 completion.

(4) *Display Information Processor (DIP) By-Pass.*—Develop an interim by-pass for the 20-year old DIP, currently used as an alternate communications routing device for the UNIVAC 1100/42. Approved and funded for April 1981 completion.

(5) *Missile Warning Display System (MWDS) Circuit Upgrade.*—Convert all the MWDS circuits to a fully coordinated (Advanced Data Communications Control Procedures (ADCCP) Protocol) configuration. Approved and funded for January 1982 completion.

(6) *Missile Warning By-Pass (MWBP) Upgrade.*—Develop a permanent replacement for the DIP ((4) above) to route critical missile warning data to the NCS and MEBU in the event of CSS failure. Approved and funded for March 1983 completion.

(7) *Off-Site Test Facility.*—Develop a complete computer facility electrically and physically separated from the NORAD Cheyenne Mountain Complex (NCMC) to develop and test software and hardware changes to the operational 427M system. Initial operational capability (IOC) was achieved on September 29, 1980, full operational capability (FOC) is scheduled for March 1981.

○