General John A. Gordon, USAF

Deputy Director of Central Intelligence

Written Statement for the

Government Readiness Subcommittee

of the Senate Armed Services Committee

February 24, 1999

Mr. Chairman, I am delighted to be here today to address a subject that is growing in importance by the day. I will be providing an overview of the Intelligence Community's readiness to deal with the Y2K problem and the potential for Y2K-related problems abroad to impact on the United States or US interests.

The Intelligence Community

Let me begin with progress the Intelligence Community is making in dealing with the Y2K problem. our objective is clear and simple: Ensure uninterrupted intelligence support to the warfighter and policymaker as we go through the Y2K transition period. Today I will review with you where we have been, our current status, and what more needs to be done.

We began to address the Y2K issue as a Community in August 1996. We elevated the seriousness of the Y2K problem to senior leadership levels. All of the IC agency directors and service intelligence chiefs take an active role in overseeing their organization's progress toward resolving the Y2K problem. We hold regular sessions of the Intelligence Community Deputies, to include the services, to address our status and issues at the Community level. Additionally, I host sessions with the Intelligence Community Principals--the heads of the various intelligence agencies--to measure and drive progress from the top and to ensure-adequate resources are applied, that we maintain the right priorities, and that we properly coordinate across agencies. The Intelligence Community is also participating in the Joint Staff CINC Operational Evaluations and is represented at the DoD Y2K Steering Committee, chaired by Dr. Hamre. Also, we are represented on the President's Council on Y2K and participate in several of the sector working groups.

we have in place an Intelligence Community Year 2000 Management Plan (June 1997) and an Intelligence, Surveillance and Reconnaissance Year 2000 Functional Readiness Assessment Management Plan (December 1998). These plans delineate organizational roles and responsibilities for fixing, testing, assessing overall readiness, coordinating, and reporting on Y2K.

Additionally, our Intelligence Community Information Systems Strategic Plan addresses activities throughout the Y2K transition period, as well as follow-on

actions that will be required after January 2000. Each of these plans was done in full coordination with our DoD counterparts.

Readiness Status

As a Community, we are tracking the progress of 1508 systems. Of these, 546 are considered Mission Critical. Mission Critical are those systems that are indispensable to the core function of an organization, without which significant interruption of the intelligence mission would occur. One example of a mission critical system would be DIA's Military Integrated Data Base (MIDB). The MIDB contains finished intelligence data on foreign nations' military and civil infrastructure (roads, telecommunications, petroleum, etc.), military orders of battle (strengths of military components, numbers of ships, tanks, etc.), and command and control structures. 138 of these 546 Mission Critical systems are to be retired during 1999, leaving 408 systems as we go into the Y2K transition. (A system is defined as an aggregation of hardware, software, and firmware applications, which together make up a particular function.) Of the 408 systems, 247 systems are fully Y2K compliant, tested and now in day-to-day use. Another 97 are fixed and tested and are in the process of being fielded to Community locations. Therefore, 85% of the Intelligence Community's Mission Critical systems are fixed or currently being fielded. Of the remaining 64 systems, 38 are in testing. These 64 systems that are behind our selfimposed December 1998 milestone for completion of fixes have been receiving senior-level scrutiny since last summer. We have gone to significant lengths to apply funding and staff resources to accelerate fix and fielding schedules wherever possible. At this time, we anticipate that 47 of the 64 systems will be fixed by 31 March 1999, the OMB target date, and that the remaining 17 systems will be fixed by July 1999. These 17 systems will not meet the OMB target date for a variety of reasons. Some have been under contract for several years with specified delivery dates after 31 March 1999 and to negotiate an earlier date would have been cost prohibitive. Some of the systems are dependent upon commercial applications that were not delivered until recently, and now the whole system must be integrated and tested. And others are so complex that the,extra time is needed to fix them.

All of these 408 M'Ission Critical systems have or will have Contingency Plan@ in place by 31 March 1999. These plans address both the prospect that a given system will not be ready by January 2000 and for the contingency that a system is thought to be ready but fails.

As we complete the work of fixing Mission Critical systems, we are not losing sight of the non-Mission Critical systems. Non-Mission Critical are those systems that will not cause significant degradation to an organization's core intelligence mission capability in the event of a failure or interruption of service. An example of a non-mission critical system is CIA's Congressional Affairs Tracking System (CATS). This application is a management tool used to report topics of interest and status of action items to our Congressional Oversight Committees. Of the 308 nonMission Critical systems that are not fully compliant, 102 are in process of being fielded, leaving 206 which are in stages of fix and testing. These non-Mission Critical systems are important to us since many are essential to maintaining smooth intelligence operations, including such basic things as ensuring that intelligence personnel are paid on time. The target to complete these fixes is 31 March 1999. I anticipate that there will be some systems that do not make this date, and we have already assessed the impact and have begun contingency planning.

Shiftina Emphasis

As we are less than a year from the first critical Y2K milestones, our attention has begun to shift significantly to risk management. This involves preparations to not only ensure we have solved Y2K problems correctly, but to make sure contingency plans are in place and shared with partner organizations as well. This encompasses three initiatives: First, we are preparing an overall mission-oriented readiness assessment; second, we are working at the Community-level for contingency planning; and, third, we have begun planning for crisis operations during Y2K's potential problem intervals, such as the transition from 31 December 1999 to 1 January 2000, as well as 28-29 February and 29 February-I March due to the fact that 2000 is a leap year.

The Intelligence, Surveillance and Reconnaissance Readiness Assessment is a functional evaluation of our Community's success at fixing the Y2K problem. This initiative is closely linked to the DoD Commanders in Chief (CINCS) Operational Evaluations that are in the planning and early execution phases. As indicated earlier, not all of the Mission Critical systems are fully compliant at this time, so--as the CINCs begin their operational evaluations--we are doing one of three things: deferring the system test until the backup test phase, testing the contingency plan, or providing a product such as archived data instead of a real time data input. Key for the Intelligence Community is the joint US Central Command, Space Command and Transportation Command operational evaluation in April. In addition to participating in the CINC evaluations, we are using their requirements to assess our Community's supporting processes and systems readiness. We will also conduct national-level assessments to ensure continued support to National Command Authority requirements. our readiness assessment activities are targeted to begin this spring and last through the summer.

The second major aspect of our risk management effort is contingency planning. Most of the effort to date has been by individual agencies aimed at their own systems-level preparations. Now, we are planning at a Community-level not only from the perspective of our intelligence system-ofsystems, but also as it relates to our basic infrastructure, such as commercially-provided power, water, and telecommunications to ensure the intelligence mission will be sustained in the event that there are significant losses of infrastructure or information technology capabilities. The challenge here is to coordinate common, realistic planning assumptions across our diverse community of providers and consumers.

Finally, the third piece of our risk management effort is crisis operations. Throughout the Intelligence Community, we have Alert Centers which monitor and respond to international events. Additionally, most organizations have some form of Systems Operations Centers, addressing problems that arise with their computer systems and networks. Both types Of centers are preparing for the potential implications of Y2K, whether they be international or domestic. We are strengthening the communications processes between centers. We are preparing for the potential that there may be many situations erupting worldwide and within our own systems environment. We are developing a Community-level monitoring, notification, prioritization, and tasking mechanism which may be required if multiple significant events occur. Other aspects we are examining are: alternate sites of operation, redundant crisis communications, crisis response teams, and visibility into all levels of contingency planning efforts.

Conclusions

In sum, Mr. Chairman, the Intelligence Community has stepped up to the challenge of the Y2K problem, which threatens our ability to continue mission critical support to our consumers. While several critical systems have not fully completed repairs, Community and agency leadership are aggressively managing

their attack on the problem and have contingency plans in place should the need arise.

Risk management is the theme of the day. We have instituted an intense, cross-Community test and assessment program to ensure we will be able to support our customers. In the event that there are failures, as there are bound to be with a problem of this magnitude and complexity, we will have,contingency plans in place to ensure that there will be no interruption to the critical aspects of the intelligence support mission.

Foreign Y2K Readiness

Now, Mr. Chairman, I would like to turn to the understanding that the Intelligence Community has about foreign efforts to deal with the Y2K problem. All countries will be affected--to one degree or another--by Y2K-related failures. Global linkages in telecommunications, financial systems, air transportation, the manufacturing supply chain, oil supplies, and trade mean that Y2K problems will not be isolated to individual countries, and no country will be immune from failures that may occur in these sectors. Fixing the Y2K problem is labor and time intensive, as well as expensive. Current Gartner Group estimates of global expenditures needed to fix the problem are on the order of one to two trillion dollars.

Ineed to say at the outset, Mr. Chairman, that there are significant information gaps that make it difficult for us to assess how serious the Y2K problem will be around the world. In many cases, foreign countries only recently have become aware of the problem and begun to examine their critical infrastructure systems for potential Y2K failures. In comparison, the United States has made a significant effort to identify and redress Y2K problems, and it was only after the process was well underway that it was possible to get a good appreciation-of the extent of the problem and its implications. Many foreign countries, particularly those that are the furthest behind, have not made such an effort, so--for our part--we can identify their likely problem areas but cannot make confident judgments at this point about what is likely to happen. Our assessments will change as more information becomes available, as countries become more aware of and deal with Y2K issues, and as incidents of Y2K failure become apparent. I will highlight those problem areas that I think have a significant chance of affecting US interests. These include, among others, foreign military systems, trade, and the oil and gas sectors, all of which I will elaborate on.

The consequences of Y2K failures abroad will range from the relatively benign, such as a localized inability to process credit card purchases by computer, to problems within systems across sectors that will have humanitarian implications such as power loss in mid-winter. The coincidence of widespread Y2K-related failures in the winter of 1999-2000 in Russia and Ukraine, with continuing economic problems, food shortages, and already difficult conditions for the population could have major humanitarian consequences for these countries.

Foreign countries trail the United States in addressing Y2K problems by at least several months, and in many cases much longer. Y2K remediation is underfunded in most countries. We have few indications that countries are undertaking contingency planning for recovery from Y2K failures:

- Time and resource constraints will limit the ability of most countries to respond adequately by 2000.

- Governments in many countries have begun to plan seriously for Y2K remediation only within the last year, some only in the last few months, and some continue to significantly underestimate the cost and time requirements for remediation and, importantly, testing. Because many countries are way behind, testing of fixes will come late, and unanticipated problems typically arise in this phase.
- The largest institutions, particularly those in the financial sectors, are the most advanced in Y2K remediation. Small and medium-size entities trail in every sector worldwide.
- Most countries have failed to address aggressively the issue of embedded processors. While recent understanding is that failures here will be less than previously estimated, it is nevertheless the case that failure to address this issue will still cause some highly dependent sectors with complex sensor and processing systems to have problems, centered right on the January 1 date.
- The lowest level of Y2K preparedness is evident in Eastern Europe, Russia, Latin America, the Middle East, Africa, and several Asian countries, including China.

Although Western Europe is in relatively better shape than most other regions, European awareness of and concern about the Y2K problem is uneven, and the Europeans lag the United States in fixing their problems. European attention was focused on modifying computer systems for the European Monetary Union conversion, which was implemented successfully on 1 January, but this was done, in many cases, by postponing coming to grips with Y2K problems.

The Asian economic crisis has hampered the Y2K remediation efforts of most of the Asia-Pacific countries. While the lines of authority for Chinals Y2K effort have been established, its late start in addressing Y2K issues suggests Beijing will fail to solve some, but not many of its,Y2K problems in the limited time remaining, and will probably experience failures in key sectors such as telecommunications, electric power, and banking.

Russia has exhibited a low level of Y2K awareness and remediation activity. While the Russians possess a talented pool of programmers, they seem to lack the time, organization, and funding to adequately confront the Y2K problem. The $3 billion estimate earlier this month from Alexander Krupnov, Chairman of the Russian Central Telecommunications Commission, is six times the original estimate. Frankly, we do not know how they arrived at this number.

One issue we are watching in Russia relates to vulnerability of Soviet-designed nuclear plants in Central and Eastern Europe and Russia to Y2K-related problems. Our analysts have done a systematic analysis of the most dangerous foreign reactors, and some of the former Soviet models are the worst. US nuclear reactor specialists know a great deal about the design and safety of these reactors, but they do not yet know what specific Y2K problems they may have. DOE specialists have been heavily involved in the process of helping US reactors overcome Y2K problems, and this process has required long and very detailed work using extensive documentation of how these reactors work. In comparison, documentation for Soviet-model reactors is poor, and no comparable effort has yet been made to trace potential Y2K failures.

We envision two ways in which potential problems with ,Soviet-designed reactors could evolve. The first involves the operation of internal components or sensors crucial to the operation of the plant, being affected or degraded by Y2K problems. For example, a valve with a digital controller designed to

automatically adjust the flow of cooling water, could potentially malfunction because the digital controller does not recognize the year 00. The second involves problems arising from the loss of off-site

power to the reactor due to Y2K problems in the power grid. This could lead to a series of Y2K problems possibly occurring simultaneously, presenting an even greater challenge to the reactor operators. While loss of electric power would in itself normally result in reactor shutdown, that process could potentially be complicated if internal Y2K problems arise within the reactor complex itself. There are digital controllers in some of the reactors that are used to drive pumps, valves, backup diesel generators, or other equipment crucial to the shutdown process. These controllers would have to work in order to ensure safe reactor shutdown if off-site power were lost.
While some Soviet-designed reactors are less vulnerable to problems from Y2K failures due to safety improvements incorporated into their designs, other reactors currently in use in Russia and other former Soviet states and allies, such as the remaining reactor at Chernobyl, are of more concern. While DOE has initiatives underway designed to assist the Russians in reducing the risk of Y2K-related reactor safety issues, the Russians have been slow to accept our help. DOE is sponsoring a study at Pacific Northwest Laboratories to identify the most likely Y2K failures in Soviet-designed reactors from internal Y2K problems or from electric power grid problems--and to assess the implications of potential failures.

Russia's Gazprom Natural Gas Pipeline network, which supplies over one-third of Europe's natural gas, also is susceptible to potential Y2K outages. Russials ability to transport and export natural gas could be interrupted in mid-winter. Potential problems include:

- Soviet-era mainframes--roughly equivalent to the IBM 360 and 370 series--have been used in Gazprom's pipeline operations centers and are highly likely to contain Y2K vulnerabilities.

- Gazprom uses supervisory control and data acquisition (SCADA) systems to monitor and control some pipeline operations. Nearly all SCADA systems purchased prior to the late 1990s contain some degree of Y2K vulnerability.

- Satellite ground stations used to transfer data between gas-producing regions to Gazprom's headquarters may have Y2K problems.
- Several hundred unattended equipment stations along remote Siberian' sections of Gazprom's pipelines may rely on vulnerable embedded processors. While most of these should work, they all need to be tested to ensure their reliability. These stations are used to relay communications and may be used to control pipeline valves. Many of them are accessible only by special convoys or helicopter, and under normal circumstances are only visited twice per year. Compressor stations--over six hundred of which pump gas through the pipeline network--also contain embedded processors that could be vulnerable.

Military systems and their command and control are particularly information-technology dependent, and thus potentially vulnerable to disruption if Y2K problems are not adequately addressed. We have been attentive to the possibility that foreign strategic missile systems, particularly in Russia and China, may experience Y2K-related problems. missile-related concerns involve the vulnerability of environmental control systems within silos to Y2K disruption. Sensors and controllers-need to be Y2K safe. Li@id-fueled missiles within silos must be monitored for fuel leaks. Optimum temperature and humidity levels must

also be maintained within the silos. I want to be clear that while local problems are foreseeable, we do not see a problem in terms of Russian or Chinese missiles automatically being launched, or nuclear weapons going off, because of computer problems arising from Y2K failures. In fact, we currently do not see a danger of unauthorized or inadvertent launch of ballistic missiles from any country due to Y2K problems.

Based on our analysis, we think the Russians may have some Y2K problems in the early warning systems that they use to monitor foreign missile launches, and at their command centers. These could lead to incorrect information being provided by such systems, or system outages. DoD has been engaging the Russians for months on these problems. A DoD delegation visited Moscow last week to help the Russians get up to speed on potential Y2K-related nuclear early warning problems.

Regarding world trade and oil, some of our most important trading partners--including China and Japan--have been documented by, among others, the Gartner Group, as behind the US in fixing their Y2K problems. Significant oil exporters to the United States and the global market include a number of countries that are lagging in their Y2K remediation efforts. Oil production is largely in the hands of multinational corporations in the oil-producing countries, but this sector is highly intensive in the use of information technology and complex systems using embedded processors, and is highly dependent on ports, ocean shipping, and domestic infrastructures. Y2K specialists have noted that world ports and ocean shipping are among the sectors that have done the least to prepare for the Y2K problem.

One additional issue I want to raise is that many foreign officials and companies who are aware of Y2K problems are looking to the West, particularly the United States, for help and technical solutions. In some cases, we have information that foreign companies or governments may blame the United States and other foreign vendors for problems in equipment and thus seek legal redress for their failures.

In closing, let me note that today we are closely monitoring a broad range of countries and sectors worldwide in terms of their susceptibility to disruption by Y2K failures. We are gathering information from all branches of the US Government, industry sources, a vast array of open sources (including hundreds of Web sites), and our own intelligence collection efforts so that we can accurately predict failures abroad and assess the implications. We are working very closely with the rest of the government, through the President's Council on Year 2000 Conversion, and will continue to share relevant information on the Y2K situation abroad. As our collection continues, and awareness of and reporting on Y2K problems abroad increases, our estimates of the type and extent of failures we are likely to see around the world will become more precise.

Mr. Chairman, the Intelligence Community is aggressively attacking the Y2K problem. While we have not met every deadline, I am highly confident that we will have fixed, tested, and deployed systems to avoid or work around the problem. Every system will be tested. Every interconnection will be tested within the Community and with our customers. But, Mr. Chairman, I am equally certain that there will be an unforeseen problem that will jump up and bite us on New Year's Day. We must and will be prepared to respond aggressively to that near certainty.