FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1447041-000

Total Deleted Page(s) = 1
Page 77 ~ b3; b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 07/16/1999

To: National Security

From: NSD
NIPC/CIOS/CIU
Contact: SSA [redacted] (202)324-0331

b6
b7C
b3
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

7/19/99 [redacted]

Title: Y2K;
NIPC MATTERS

Synopsis: To request the initiation of an umbrella case for FBIHQ to utilize in connection with the coordination a various activities and preparing communications related to Y2K.

Details: A Y2K Crisis Action Team (CAT) has been formed to address Y2K related activities and coordination for NIPC. This team will be preparing communications to the field and formulating contingency plans to be implemented when the millennium date change occurs.

This umbrella case, "Y2K" will be utilized to coordinate these activities and serve as a central point for communications and Y2K related data.

♦♦ [redacted]

b6
b7C
b3
b7E

UPLOADED BY [redacted] 7/19/99

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 08/30/1999 **Date:** 07/01/1999

To: All Field Offices **Attn:** All SACs
NIPC Coordinators
Key Asset Coordinators

From: National Security
CEST/CIOS/NIPC, Room 11719
Contact: [redacted] (202) 324-0331

b6
b7C
b3
b7E

Approved By: [redacted] 11/5/99

Drafted By: [redacted]

Case ID #: ~~66F-HQ-A1276902-SUB A-1-30~~ (Pending)
294I-HQ-1270744-23

Title: NIPC Y2K Cyber-Crisis Action Team;
Field Office Cyber-Crisis Contingency
BUDED: 8/30/1999

Synopsis: To provide guidance for Y2K Cyber-Crisis Contingency planning and response and to request initiation of contingency planning for the Field Offices.

Details: Presidential Decision Directive (PDD) 63, Critical Infrastructure Protection, states "The National Infrastructure Protection Center (NIPC) will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means of facilitating threats and monitoring reconstitution efforts." The National Infrastructure Protection and Computer Intrusion Program (NIPCIP) implements this national responsibility and assigns

investigative and response activities to the National Infrastructure Protection Computer Intrusion (NIPCI) squads/teams in FBI Field Offices.

In order to fulfill this national responsibility, the NIPC has established a Y2K Cyber-Crisis Action Team (Cyber-CAT) and is developing and coordinating Y2K cyber-crisis contingency planning within the FBI and with other Government Agencies.

The potential Y2K cyber-crisis event is unique from other incidents/emergency situations/crisis in that:

a. It could be an event of truly national scale because it may simultaneously affect multiple areas throughout the nation.

b. While we know the "when" of Y2K, we do not know the combined or possibly cascading effects of Y2K with high certainty throughout different time zones and different infrastructures; geographically dispersed.

c. Y2K effects may overlap to some degree with existing cyber/infrastructure problems; we may not immediately be able to discriminate a Y2K-caused problem from a "normal" cyber or infrastructure problem.

The NIPC is developing methods and procedures for the Field Offices to use in assessing and reporting incidents during the Y2K period: what is expected; what is possible; what to look for; what and how to report. This is expected to be delivered by the NIPC Y2K Cyber-CAT by October 1999, and will be provided by a separate communication. These procedures will include methods by which an initial assessment can be made to determine whether an incident is maliciously induced, as opposed to a Y2K software anomaly incident not under the responsibility of the FBI.

Contingency Plans for Y2K events:

A. Identification of Y2K POC's and Command Posts:

Each Field Office is requested to identify and compile point of contact (POC) information for law enforcement and emergency response entities that are located in their Division, and determine if these entities will have a Y2K command post. Each Field Office should identify the method/procedure to contact these command posts.

To assure uninterrupted operations, each Field Office should also identify the following information for Y2K cyber contingencies:

1. Key Field Office resources that are required to support "critical missions" (i.e., electricity, telecommunications, etc...);

2. Field Office supplies that will be necessary to have on hand for meeting critical mission requirements, including cash for emergencies; and

3. A current POC in each Field Office for NIPC/Y2K related activities. This POC should be the focal point for Y2K communications connectivity and planning. This point of contact should be an individual who is an SSA or SA assigned to a squad/team or individual(s) responsible for NIPCI investigations. NIPC will compile and maintain a comprehensive list of the POC's and provide it to all Field Offices with additional Y2K data at a later time.

B. Y2K Contingency Communications:

The NIPC will place an assured, secure communications package in each Field Office. This equipment package is for the NIPCIP program for Y2K connectivity with the NIPC Watch and Warning Unit at FBIHQ. This is predicated upon approval of funds. Minimal facilities impact or Field Office overhead is envisioned; however, b7E

Locally, will be required for secure communications FBIHQ will be in communication with other Government agencies to assist in investigations or provide additional POC's for investigative information as needed. In the near future, the NIPC will be sending out communications regarding guidance on the use, implementation and procedures for the equipment being sent to the Field Offices.

C. Develop a database for cyber-incidents:

To prepare for this potential "scheduled crisis," the NIPC will require Field Office assistance to complete initial planning activities. In addition to this communication, the Key Asset Program will be tasking the field to collect and provide POC information for Key Assets,

[redacted] and POC information for [redacted] Key Assets [redacted] b7E

[redacted] The information collected will be maintained in the [redacted] To alleviate duplication of effort, the information collected and input into this database will be used by the NIPC/Y2K command post at FBIHQ. Other requested information will include copies of the Key Asset Y2K contingency plans and Y2K POC's if available.

At the same time, Field Offices should also compile a database of "cyber partners" (law enforcement and counterintelligence agencies, emergency services providers, computer emergency response teams, telecommunications systems, ISP's, and infrastructure liaison POC's). Other local and regional resources such as [redacted] corporate Chief Information Officers and officials from the information technology sector, computer network professional organizations, and university computer science departments can be invaluable in providing critical guidance or support both before and during a crisis. These POC's should be cultivated as part of the normal planning process. The database should include primary and alternative communication methods and include both local and remote (i.e., national headquarters, etc.) command posts and POC's.

D. Local Y2K Planning:

Each Field Office should prepare a Y2K Contingency Plan. This should cover, as a minimum, a manning schedule between December 27, 1999 and January 15, 2000; current emergency contact lists; hours of operation; dates of operation; and procedures to be followed for cyber-related crisis event occurrences. It is anticipated that events and reporting will be handled through normal investigative procedures. **In the event that a Y2K cyber-crisis does occur, all infrastructure cyber events should be reported to the NIPC Y2K command post.**

1. Field Office Y2K Responsibilities:

Because Y2K has the potential of affecting multiple areas on a national scale, each NIPCIP Squad (Atlanta, Boston, Chicago, Charlotte, Dallas, Los Angeles, New Orleans, New

York, San Diego, San Francisco, Seattle, WFO) should have NIPCI personnel staffed and available on a 24-hour basis beginning no later than December 31, 1999, and continuing through January 2, 2000. All other Field Offices should evaluate whether they need to have personnel available on a 24-hour basis when the millennium date change takes place. The Public's perception of Y2K and Y2K-related incidents has the potential to generate an increased amount of complaints and inquiries. Each Field Office should be prepared to handle complaints and coordinate with NIPC Command post at FBIHQ and other local and federal emergency agencies, including the Federal Emergency Management Agency (FEMA). Each Field Office should have a call-out plan in place for personnel and a clearly defined leave policy regarding the year-end time frame.

Each office is requested to provide a manning schedule that identifies staffing time, and the number of personnel assigned and available, and the positions (SA, SSA, Computer Specialist) of the personnel.

E. Method and Format of Reporting Information Requested:

1. Field Office Y2K POC information should include but not limited to: Name, position or title, e-mail, phone number, pager number, fax number, and alternative communications, etc ...;

2. Law enforcement POC information, Y2K contact information to include but not limited to: Name, position or title, e-mail, phone number, pager number, fax number, and alternative communications, etc ...;

   If a local law enforcement entity is standing up a Y2K command post or emergency operations center provide structure to include but not limited to: Telephone number, fax number, e-mail, number of people, hours of operation, and dates of operation; and

3. Cyber partners information to include but not limited to: Name, position or title, e-mail, phone number, pager number, fax number, and alternative communications (this should be only information that will not be included in the Key Asset database).

4. Field office staffing plan to include: Days/hours of Y2K response, and number, position and title of personnel assigned.

This information should be provided, preferably via digital or software form, to [redacted] at 202-324-0331/0322, respectively; or fax to 202-324-0311, no later than August 31, 1999. b6 b7C

LEAD(s):

Set Lead 1:

ALL RECEIVING OFFICES

Identify point(s) of contact within the Field Office for NIPC/Y2K issues. This POC should be an individual who is an SSA or SA assigned to a squad/team or individual(s) responsible for NIPCI investigations.

Set Lead 2:

ALL RECEIVING OFFICES

Identify and compile point of contact information on law enforcement entities that are located in their Division and determine if they will have a Y2K command post.

Set Lead 3:

ALL RECEIVING OFFICES

Develop a "cyber partners" database for Y2K cyber-incidents.

Set Lead 4:

ALL RECEIVING OFFICES

Identify and procure supplies that would be necessary to stockpile to assure meeting critical mission requirements.

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 07/22/1999

To: National Security

From: National Security
NIPC/CIOS/CEST
Contact: SSA [redacted] (202) 324-6234

b6
b7C
b3
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] Pending)

Title: Year 2000 (Y2K)
Crisis Action Team (CAT)

Synopsis: To document for the file, receipt of the Report of the Defense Science Board Task Force on Year 2000, dated April 1998.

Enclosure(s): Attached to this document is a copy of the Report of the Defense Science Board Task Force on Year 2000, dated April 1998.

Details: The purpose of this communication is to act as a transmittal of attached enclosure to the Y2K CAT file. A copy of this document has been disseminated to the following individuals:

b6
b7C

[redacted] - Unit Chief, Computer Investigations Unit
[redacted] - Acting Unit Chief, Special Technologies and Applications Unit
[redacted] - Unit Chief, Outreach and Field Office Support Unit
[redacted] - Unit Chief, Analysis and Information Sharing Unit
[redacted] - Unit Chief, Watch and Warning Unit
[redacted] - Relief Unit Chief, Cyber Emergency Support Team
[redacted] - Y2K CAT Team Leader
[redacted] - Y2K CAT Member

♦♦

UPLOADED BY [redacted] 8/27/99

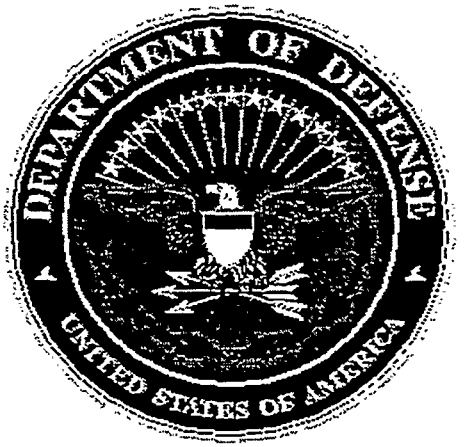
REPORT OF THE

DEFENSE SCIENCE BOARD

TASK FORCE

ON

Year 2000



April 1998

OFFICE OF THE UNDER SECRETARY OF DEFENSE
FOR ACQUISITION and TECHNOLOGY
WASHINGTON, D.C. 20301-3140

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

2 APR 1998

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (ACQUISITION & TECHNOLOGY)

SUBJECT: Report of the Defense Science Board (DSB) Task Force on Year 2000

In response to tasking from the Under Secretary of Defense (Acquisition & Technology), the DSB Task Force on Year 2000 has examined the Department's efforts and prepared the attached report.

The Task Force concluded that the Year 2000 problem is a very serious one, but more than just a CIO problem. It is a CEO problem and it needs direction and guidance from the top. Its solution must include all users of IT, including the Secretary, Chairman, and the warfighting CINCs.

The Task Force made three major recommendations:

- USD(A&T) appoint a full-time executive
- OSD establish a Year 2000 "escape valve" fund for the FY99 budget
- OSD should work with the components to establish incentives for Program Managers.

These steps must be taken to get on top of the problem and reduce the management risk.

Craig Fields
Chairman

Attachment

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

30 MAR 1998

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Report of the Defense Science Board Task Force on Year 2000

Attached is the final report of the DSB Task Force on the Year 2000. This Task Force was asked to determine if the priorities assigned, resources allocated, and funding strategy used to implement the Department's Year 2000 program are sufficient.

The Summary Findings of the Task Force are:

-- The Y2K problem is a very serious one; it is a big system and system management problem. DoD is experienced and capable in analyzing, structuring and managing such programs.

-- Further, Y2K is a CEO problem, not just a CIO problem; it needs direction and guidance from the top; its solution must involve all users of IT which certainly includes the Chairman and the CINCs as well as the more traditional users.

The Task Force makes three major Recommendations:

1. USD(A&T) should appoint a full time executive with the requisite authority and staff to provide the needed leadership and the overall plan for addressing the Y2K problem. Specific tasks to insure that each area is following a disciplined approach, is getting reliable support and has reasonable consistency with the rest of the Department are delineated.

2. OSD should establish a Y2K "escape valve" fund under the direct control of the Y2K executive to be made available for certain special needs. Funds should be established now and also put into the FY99 budget.

3. OSD should work with the components to establish strong incentives for program managers and the other key people to provide the necessary attention and emphasis to the Y2K issue.

The Task Force believes the Department needs to take these steps to get on top of the Y2K problem and to reduce substantially the risks associated with these problems.

The Task Force, its advisors and its support staff consisted of an exceptionally competent group of dedicated individuals. It was a pleasure to work with them.

Charles A. Fowler
Task Force Chair

David R. Heebner
Task Force Vice Chair

Attachment

Table of Contents

List of Tables

Executive Summary

Most, but not all, of the problems associated with computer systems' calendar date format and the coming year 2000 are due to the use of a two digit year designation in which the year 2000 will become 00 and be interpreted as 1900. This could cause computers to quit functioning or produce incorrect data outputs, which could result in problems such as incorrect calculations of pay and retirement, mis-pointing of directional antennae, erasure of data fields, and rejection and return of "old" items.

Within DOD, the ASD (C^3I), as Chief Information Officer (CIO), has been responsible for the development of the DOD Y2K Action Plan [January 1997] and the DOD Management Plan [April 1997]. These include a five-phase process covering Awareness, Assessment, Renovation, Validation, and Implementation. An initial effort to identify Mission Critical [MC] systems on which to focus resulted in over 3,000 computers being labeled MC. This is because MC systems were defined as being those whose degradation would cause a loss of a core capability. Brief probing by the DSB Task Force suggests that by applying the "so what" test, the number of "priority MC system" could be reduced by a factor of 10 or greater.

In the current DOD management of the Y2K problem, policy and oversight are centralized in OSD, while execution is decentralized to the component Services, CINCs, Agencies, etc. Each component is funding Y2K fixes out of existing budgets — a so called "take-it-out-of-hide" approach. Information on each MC system is listed in the Defense Information Support Tools (DIST), and DOD has a goal of fielding and testing all MC systems by November 1998 to allow a full year to work out the bugs.

The Task Force feels the current management approach has problems in that status reporting is too general, lacks measurable references to any program plan, and lacks enforcement of "exit/ entrance" criteria. Despite the fact that industry and commercial concerns view the Y2K problem with alarm, DOD components report no difficulty in meeting compliance by 2000, and have focused little attention on promulgation of "fixes," risk management, or development of contingency plans. Program managers and other key people have no specific incentives to give the Y2K problem priority over other issues, especially system performance improvements.

The Task Force believes that the Y2K problem is a major system management problem, capable of being solved with DOD experience in analysis, structure and management of programs. The key is that DOD recognize that Y2K is a CEO problem, not just a CIO problem, and that DOD needs direction and guidance from the top. Any solution should involve all users of IT, and should certainly include the Chairman and CINCs as well as more traditional users.

The Task Force makes three major recommendations, the first of which is the appointment of a full time executive with requisite authority and staff to provide the needed

leadership and overall plan for addressing the Y2K problem. The Task Force has delineated specific tasks to insure that each area is following a disciplined approach, is getting reliable support, and has reasonable consistency with the rest of DOD. These tasks include identification of really Mission Critical systems, management, testing, Information Warfare [IW] vulnerabilities, and a host of other responsibilities.

Secondly, the Task Force recommends the establishment by the Office of the Secretary of Defense (OSD) of a Y2K "escape valve" fund under the direct control of the Y2K executive to be made available for certain special needs. These funds should be established now and put into the FY99 budget.

Thirdly, the Task Force recommends that OSD work with the components to establish strong incentives for program managers and other key people to provide the necessary attention and emphasis to the Y2K issue.

It is not possible to foretell precisely the total impact of Y2K problems on DOD operations. However, the U.S. has sized and equipped its forces predicated on overwhelming information superiority and this is widely known. The risk of being unable to operate effectively and efficiently during any crisis that might occur during the transition period is sufficiently serious that prudence demands that DOD take those steps needed to reduce that risk substantially. The Task Force believes that the measures it has recommended are necessary and appropriate for such risk reduction.

I. Introduction

The Year 2000 (Y2K) Task Force was formed at the request of the USD(A&T) to review the issues the DOD faced in dealing with the technological problems associated with the arrival of the Year 2000, frequently referred to (erroneously) as the beginning of the next Millennium.

The Terms of Reference (TOR) are shown in Appendix A. The members of the Task Force, Government Advisors, and supporting staff are listed in Appendix B.

A. Current Program

1. The Problem

Since the beginning of the information age [circa 1950] no standardized calendar date format has been used — more than twenty formats have evolved, most of which do not accommodate the century change.

The DOD uses computers; including embedded computers and control devices, to perform or support: business functions [financial and personnel management, health care, contract management, and logistics management], strategic/ tactical operations [mobilization, deploying, and maneuvering forces and weapons systems used by the forces], and intelligence, surveillance and security efforts.

Most, but not all, of the problems are due to the long-standing use of a two digit year designation. Thus year 2000 will become 00 and be interpreted as 1900, which can cause computers and control devices with date microchips to quit functioning or produce incorrect data outputs. Some of the many possible impacts follow: some systems won't work at all; incorrect calculations of pay; incorrect retirement dates and interest; assumption of 1900 satellite ephemeredes and associated mis-pointing of directional antennas; erasure of entire data fields; and rejection and return of "old" items.

This may be looked at as an excellent example of self-inflicted information warfare!

2. DOD Approach

The White House Office of Management and Budget [OMB] is in overall charge of the Federal government Y2K efforts and the DOD reports progress to OMB on a regular basis.

ASD (C^3I), the DOD Chief Information Officer [CIO], has been responsible for developing and publishing the DOD Y2K Action Plan [January 1997] and the DOD Y2K Management Plan [April 1997].

The process for addressing the issue consists of five phases: Awareness, Assessment, Renovation, Validation and Implementation. An early step in the process is to identify Mission Critical [MC] systems. The effort thereafter focuses on MC systems. The current definition of an MC system is one whose degradation would cause a loss of a core capability. This definition led to a large number [several thousand] of systems being listed as MC. A tighter definition is being devised now which will make some reduction [probably 20-30 percent] in the number systems listed as MC. The DOD goal is to have all MC systems totally fielded and operationally tested by December 1998, thereby giving a full year to wring out all the bugs.

The DOD management approach consists of the following:

- Centralized Policy and Oversight by OSD
- Decentralized Execution by the Components [Services, JCS/CINCs, Agencies]
- Resources: No identified DOD funding; each component will fund Y2K work out of existing budgets; a "take it take-it-out-of-hide" approach
- Information on each system being worked [except, as noted later, the intelligence systems] is listed in the Defense Information Support Tools (DIST).
- There are frequent meetings and status reports. Much of this reporting is required for the quarterly report to OMB. Some additional reporting is required to OSD.

The 3rd quarter, 1997 report showed:

Total systems Identified			25,054
Mission Critical			3,143
Compliant			*672
Being replaced			203
Planned Terminations			128
To repair			2,140
	In Assessment	148	
	In Renovation	1,045	
	In Validation	605	
	In Implementation	305	
	Completed repair	37	
	Total	2,140	

*But Not Proven

Table 1 — Y2K Statistics

The focus of DSB and OMB attention has been on the 3000 plus so -called "Mission Critical" systems

3. Status: Good News

- There is now top level interest and concern with the Y2K problem in DOD with the Secretary, the Deputy Secretary, the Chairman, the Department Secretaries and Agency Heads receiving regular reports.
- Much good work has been and is being done in many places.
- Many old legacy systems are being replaced.
- Most weapon systems do not have serious "date" problems BUT many of the systems they interface with do. Also, the hardware used by some systems may have embedded "date" problems that are not apparent from examining the software alone.
- The efforts in the DOD medical community are impressive and probably ahead of the civilian community. There are, however, some issues that need addressing as noted later.

B. Task Force Approach

The task Force held a series of meetings, the dates and agendas of which are presented in Appendix C. Panels were formed to gather more detailed information — the members and leaders of the panels are found in Appendix D. Briefings and visits made by the panels are shown in Appendix E. Section II, that follows, consists of the reports from the panels

The Task Force as a whole developed a number of Observations, Concerns, and Findings, based on the meetings and reports and presented in Section III. These formed the basis of the Recommendations listed in Section IV.

II. Specific Areas Reviewed

A. The DOD Process and Resources

The following paragraphs deal with the monitoring of ongoing Y2K activities, the prioritization of mission critical systems, and resource utilization, all of which are essential in assuring that the process is managed efficiently, thoroughly, and cost-effectively, while also assuring that critical milestones are met.

1. Monitoring

The only OSD level guidance dealing with the Y2K problem is the "Year 2000 Management Plan," version 1, dated April 1997, published by the Assistant Secretary of Defense (ASD) for Command, Control, Communications, and Intelligence (C^3I), Information Technology Directorate. This Management Plan calls for a "central policy and decentralized implementation" with responsibilities distributed across the various services, programs and agencies within DOD.

While the Plan defines generic steps to be taken by DOD organizations to identify systems needing remediation, checklists to assure compliance, and includes formal reporting mechanisms, it lacks a unified, overall schedule, milestones, risk mitigation strategy, and designated anticipated resources required to execute the activity. There also does not appear to be any SECDEF level guidance directing subordinate agencies' compliance with Y2K performance standards, including monitoring of activity and resource utilization.

Although a progress reporting template has been established, and a significant record keeping effort is under way, it does not appear to have a solid metrics program in place to accomplish the following:

- Identify quantitative and qualitative goals at a milestone or elemental level
- Provide meaningful measures to track progress against these goals
- Define threshold indicators to trigger management actions
- Provide a tracking/ closure methodology to assure compliance and success

To remedy these shortcomings, an effort should be made to create a policy and directive to establish common objectives for the program and with other Departments of the Federal Government. Also, a mechanism needs to be put in

place to collect plans and schedules and to track execution and expenditures of resources against the plan in order to define, organize and track the progress of the disparate Y2K activities across the DOD.

The Task Force recommends the establishment of a full time executive with the requisite staff to provide the needed leadership and the overall plan for addressing the Y2K problem. The executive would reside in an Office of Primary Responsibility (OPR) appointed by the Secretary of Defense. The OPR should be responsible for the development of a comprehensive Year 2000 Remediation Plan to provide templates, schedules, milestones, tools, and performance and fiscal reporting mechanisms for effective oversight and implementation of the remediation process. The OPR needs to be given the authority to determine which systems are "mission critical" in order to assign remediation priorities. Functional user input should be sought in determining mission critical systems, and reviewed by the JCS/CINCs. The OPR should provide a standardized reporting mechanism, and be held responsible for tracking and assuring performance and compliance with the Remediation Plan.

Comprehensive test plans must be put into place linked to specific program plans and milestones. Provision for compliance audits need to be established to verify the readiness of mission critical systems, and that schedules are being met. Community of interest Project Managers should be established and held accountable for systems interface. Mechanisms for monitoring compliance of commercial-off-the-shelf (COTS) and government-off- the-shelf (GOTS) should be established, and JITC should be considered as the prime DOD organization responsible. JITC should work with GSA and other Governmental organizations in disseminating this information community wide.

2. Prioritization/ Mission Critical Systems

Over 3,000 systems have been identified as being "mission critical" — but there are indications that the current prioritization approach does not adequately identify the systems most in need of special attention. Some of the systems identified, while important (i.e., video conferencing), are not in the same class as other truly critical systems (i.e., logistics system). In some systems the manner of Y2K failure, while an inconvenience, may not preclude the system from normal basic functions.

It is possible that the number of systems identified as "mission critical" could be reduced by a factor of 10 through the application of the "so what?" test. This would allow DOD to focus on the systems that need most attention. While focusing on the really "mission critical" systems will minimize the risk to DOD's warfighting capability, it is important to note that it will not fully solve the Y2K problem. There are thousands of other systems that are important, though not "mission critical" that ultimately need to be addressed to restore full warfighting capability.

3. Resource Utilization

Currently expenditures to assure Y2K compliance will be contained within normal operating budgets. This "take-it-out-of-hide" approach seems to work well in those places where there is an ongoing program, including planned IT system replacements and upgrades. However, where no such designated funding is provided, performance accountability may suffer. With programs reporting "no bad news" or with no funding visibility, the ability to sweep the effort "under the rug" must be avoided. Systems with no defined program office or budget may not have needed funding.

The "take-it-out-of-hide" approach also provides no resources for fixing "homeless" systems (e.g., those without a program office or budget) or for the replacement of legacy systems in financially strapped areas. To date, there is no evidence of solid "Bases of Estimate" for the operational or functional units' remediation efforts. Some system developed in the "field" may not have strong configuration management, development processes, or qualified resources to remediate these systems. Perhaps most important, no funding mechanisms exist for system interface and "system-of-systems" testing.

It is not possible to estimate the total cost of addressing the Y2K problem, because remediations have not been fully estimated, the costs of ongoing activities have not been clearly identified or segregated, and testing phase cost estimates do not exist yet. Finally, funding must be provided or allocated for the period and efforts AFTER the year 2000. There will be substantial costs to address temporary fixes, to fix non-"mission critical" systems, and to implement new capabilities that were postponed either to allow work on the Y2K problem or because of the fear of introducing new problems at this critical time.

B. Management Issues

The DSB Year 2000 Task Force has had presentations from various consulting groups, to include: MITRE; Keane Inc.; Science Applications International Corporation (SAIC); Paul Strassman, Inc; Bellcore; and International Business Machines (IBM). In addition, the panel had overviews from various operating functions from within the Department of Defense.

If DOD wants and expects critical systems to work on January 1, 2000, with a high degree of probability, or if DOD needs assurance that sufficient progress is being made, then in our judgement, the DOD Y2K program lacks adequate control.

Our unease is driven by the following:

- The size and impact of the Y2K problem on operations are unclear.

- The resources committed to solve the Y2K problem are partially visible, but also partially buried in programs and operation.

- Whether a small or large fraction of technical resources is currently involved in Y2K is unknown, so surge capability is unknown.

- Commercial organizations, in finance, logistics, and transportation, are spending hundreds of millions of dollars for testing and remediation, which is much larger than visible DOD investment.

- The portfolio of Y2K efforts includes individual efforts that are very well done, and others that are unmanaged. Therefore the portfolio quality is questionable.

- Most software programs do not meet schedule originally envisioned

- The downside, or disruption, if mission critical systems are jeopardized is substantial

Three primary management issues have evolved for the Task Force and are discussed in the following sections:

- Incentives – what incentives could be used to help facilitate timely and through resolution of Y2K problems

- Replacement of Legacy Systems – what approaches could be used to encourage replacement of legacy systems increasing long term benefits to DOD.

- Promulgation of fixes – what approaches could be used to effectively share tips, processes, and software to correct Y2K problems.

1. Incentives/ Disincentives

After review and presentation by weapons system programs, functional managers and Service executives, we believe that the Y2K problem is not adequately defined, the magnitude of the solution is unclear. The consequences of failure have been defined too broadly. Operational commanders understand too little the implications of Y2K to operations. All of which raises concerns about the outcome of the project. Such conditions on a weapons system project would raise alarms, and we believe should with respect to Y2K. These conditions result in inadequate motivation down the line leading to less than desired urgency, greater uncertainty, inappropriate tradeoffs, and schedule slippage. Furthermore the current implementation of the Defense Reform Initiative may lead to further elimination,

reduction and or retirement of key personnel with the associated possible loss of Y2K knowledge and experience.

Our impressions are more true for support functions than for weapon systems, on average. We believe that:

- Objectives are too general, incomplete and only measurable at the extremes of catastrophic failure or complete success.
- Priority is a staff priority, delegated to lower levels, with regular but too infrequent reviews of progress, slippage, or risk.
- Grades of failure from catastrophic to minor need to be defined by individual system, failure modes identified, and urgency clarified.
- Organizational responsibility, instead of dispersed as broadly as it is, needs to be strongly coordinated, measured and evaluated by a powerful project group at the center.
- Resources taken 'out of hide' favor those organizations most likely to be advanced in their understanding of the problem, and disadvantage those organizations most likely to be laggard.
- Technical people will be in greater demand as testing peaks in 1998, both inside and outside of DOD. Little has been done to ensure that technical people are available as needs peak and as rapidly escalating compensation externally exerts pressure on people to retire or resign. This is particularly a worry if test results show substantial shortcomings.

Motivating a dispersed organization, with many competing priorities, is not easy. Currently, many of the lessons learned on weapon system development about project team motivation are not being rigorously applied to this equally complex project. They should be.

The Motivation sub-team has the following observations to consider. Y2K should be managed like the large, complex and potentially disruptive project that it is. DOD has great experience in managing complex projects. The lessons, skills and structure from those projects need to be applied to Y2K. The vast difference in motivation between a well organized project and a poorly organized project is understood and well known. The management techniques that create successful weapons system teams need to be applied to this project at the earliest possible time, in doing what DOD already knows what to do:

- Clarify Objectives: Although financial objectives are clear, there is a need to be clear about operational readiness, maximum tolerable disruption, extent of legacy system switching, and other non-financial objectives.

- Establish priorities: Establish Y2K as a major CINC/line priority, instead of a staff, or even more inappropriately, a CIO concern.

- Identify the consequences of failure.

- Identify more clearly the consequences of failing to correct critical, important, or support/ indirect systems, system by system. An appropriate sense of urgency can then be created for each weapons system, each operational unit, and the portfolio of systems as a whole.

- Create a project organization: Create an organization appropriate to the problem, with the power to move quickly, intervene in line organization programs where necessary, and marshal the SECDEF, USD and Chairman, JCS attention where needed. Install normal time, cost, and technical performance measures.

- Resource adequately: Insure that more than enough resources (time, money, programmers) are available for critical systems, and at least sufficient resources for important systems. Particularly review 'homeless' systems for adequate resources for few managers will be motivated to spend time and resources on testing and fixing these.

- Improve individual motivation: Within the technical community responsible for testing and fixing systems, take extraordinary steps to motivate key people through 2001, including carryover of bonuses as are being offered elsewhere to retain programmers, and acquisition of test tools without long procurement and administrative delays, and the like.

2. Replacement of Legacy Systems

Based upon information presented to date and conversations with task force members, the team has the following observations with regard to replacement of legacy systems where required within the various DOD agencies. These observations are followed by a background section on relevant issues.

a. Observations

The DOD should set aside enhanced funding, approximately $100M, to be made available for replacement of legacy systems where this is critical and other program funds are not available. Each agency, in the process of performing a Y2K assessment/ inventory of their systems, should determine whether system replacement outweighs current system fixes for the maximum in long term benefits and the minimum in risk. The various agencies should present these business cases for system replacement to the Y2K Steering Committee who would select those proposals demonstrating

the most merit. Final funding approval for implementation should be obtained by the Comptroller.

DOD should take advantage of COTS/GOTS as replacement solutions whenever practical.

b. Sources for this enhanced funding could be from the following:

1) funds earmarked for routine Operational Test and Evaluation (OT&E) for all systems;

2) funds from prior year USG contracts;

3) 85 person years of DOD IG and Service audit agencies efforts to examine status diverted to fixing Y2K problems; and

4) OSD imposed tax across some or all of the DOD budget to augment above resources.

DOD needs the ability to grant requests to carry over end-of-year funds for Y2K projects. This should include Operations and Maintenance (O&M) funds and the transfer of other funds (Research and Development [R&D] and Procurement) into O&M type activities for the purpose of fixing Y2K problems. DOD must work closely with the Comptroller and Congress to get the exemptions and permission to allow this to happen.

c. Background Findings and Issues

The goals and objectives of the DOD Y2K Management Plan encourage agencies to recognize the Y2K problem as an opportunity to retire legacy systems early. However, at issue is the fact that the services have been directed to utilize existing funds for system replacement should this be their elected Y2K solution. This "take-it-out-of-hide" approach seems to work well in those areas where there is an ongoing program including planned IT system replacements and upgrades. On the other hand, this directive has encouraged some agencies to understate Y2K issues or take the least-cost approach toward Y2K compliance which, in some cases, may not be the best long-term solution from an IT standpoint. Legacy system replacement could allow for long-term cost savings but not necessarily within the Y2K horizon.

The "out-of-hide" approach provides no resources for: fixing "homeless" systems (those without a program office, budget, etc.); replacing legacy systems in financially strapped areas; and, funding interface and "system-of-systems" testing.

The organizations with the worst "legacy system" problems are those with less knowledge, technical skill and resources. They are least able to manage and fund replacements. Likewise, they are most in need of resources and direction, from OSD. They are most likely to have problems due to old, complex hardware or software.

d. Legacy System Summary

Early Y2K testing is important to accelerate identification of those legacy systems that fail Y2K. Timing for replacement of these systems is important. Otherwise implementing last minute and costly patches may end up being the only solutions. Additionally, Y2K fixes will likely add new system "bugs" to established systems, complicating attempts to remedy Y2K problems quickly. Furthermore, as mentioned subsequently, replacement funds may be needed for financially strapped areas.

3. Promulgation of Fixes

Based upon information presented to date and conversations with task force members, the team has made the following observations with regard to promulgation of "fixes" across the various DOD agencies. These observations are followed by a background section on relevant issues.

a. The Problem

There seem to be many areas in need of management attention and there are several crucial areas where top level direction, guidance and program review are needed:

1) It is not possible to determine accurately the current status of Y2K fixing because the level of reporting is too general and lacks measurable references to any program plan benchmarks, and because few systems have entered the crucial testing phase.

2) Good program management processes do not appear to be in place to report against and, thus, realistic determination of status of the ongoing efforts is not possible.

3) Enforcement of "exit/ entrance" criteria for the several phases is lacking.

4) Almost all presentations report everything is going well and no difficulty is expected.in meeting compliance by 2000.

5) In contrast industry and commercial concerns view their problems

with alarm.

6) We seem to have the worst of both worlds with lots of reporting required of the components but little value to the reports. Although some, perhaps most, of the reporting is needed to meet OMB requirements, much could be done to make the reports more meaningful and to reduce the number of reports. Efforts are needed to automate the required reporting from the DIST and other information collection tools currently in use.

7) There has been inadequate attention to promulgation of "fixes," risk management and development of contingency plans.

8) There are no specific incentives for program managers to give the Y2K problem priority over other issues especially system performance improvements.

The DOD no longer has much clout in getting attention to their special problems since they represent a very small part of the business base of U.S. computer and software industries. Further, many of these companies seem to feel they have no responsibility for Y2K compliance of previously delivered products. High level attention would help the programs in dealing with this issue.

b. Background Findings and Issues

Y2K Project Tracking — the level of reporting on Y2K status has been too general and lacks measurable references to any program plan. A review that goes down to lower levels of the organization reflects the true status of a project is not on schedule as the briefs may indicate. At the service level, it appears there is no real analysis being done on how or why the plans on various systems are changing over time. It cannot be determined what specific systems are slipping schedule and why, which leads to the conclusion that better methods of project management need to be applied.

Effective Communications — there has been inadequate attention to the promulgation of "fixes." While working groups may function well in uncovering Y2K issues and disseminating this information within the Y2K community, it does not appear to filter down to the lower program management levels where implementation of the "fixes" to these issues is critical. Working groups tend to function as purely a reporting mechanism. A central OPR could facilitate this communication.

- Testing — promulgation of fixes efficiently will become more urgent as more organizations enter the testing phase. There is a likelihood that a "bow wave" of problems identified in test will exist — perhaps beyond available resources. Efficient promulgation will be critical to solving problems in a timely manner. Likewise promulgation of failures without fear of litigation reaction by vendors must take place.

c. The Solution

Assure effective Y2K communication is taking place across all working levels. While Working Groups may serve well as status reporting mechanisms, the DOD Y2K executive needs to ensure that the appropriate outcome of these Working Group efforts is communicated down through the proper levels, which could mean as far down as the Program Management tier.

The main promulgation vehicle that should be considered is a central web site that has all relevant information pertaining to the overall DOD Year 2000 Program Plan. Not only could this web site contain the unified, overall DOD schedule, milestones and risk mitigation strategy, but should serve as the primary sharing media for information on Y2K problems, best practices, lessons learned, COTS/GOTS Y2K compliance, Y2K tools, and for leveraging Y2K experiences across the different agencies.

The GSA comprehensive web site could serve this purpose. However, should this web site be made publicly available, there would be some vulnerabilities in regard to disclosure of DOD trouble areas, issues, or other topics considered sensitive in nature. Considering this, the web site could be structured such that only Y2K functional areas or broad categories of Y2K work efforts would be identified along with corresponding points of contact for more detailed information. This would support information access on a need-to-know basis only.

The Working Groups should be a primary source of input to the central web site. Relevant input should also be provided by the Y2K Project Office, and the Services Project Offices. Also, as the DOD Y2K executive office completes various projects throughout the DOD, they will become a vast repository of information, much of which will need to be shared via the web site. This should assist in avoiding duplicative efforts across agencies in their Y2K projects.

The DOD Y2K executive should develop a checklist for projects in each priority tier.

One successful means of maintaining a Y2K remediation schedule is to surface the unknown issues as early as possible. To accomplish this, the DOD executive, as part of its Y2K mission, should ensure in-depth analysis of schedule movement. A sample of mission critical programs/ systems should be reviewed and tested to ensure that the status being briefed actually represents the realities and issues down at the detailed program level. Not only will this ensure issues are addressed on a timely basis, but will foster more effective and accurate communication of solutions across the different agencies.

C. Testing, Emergency Response, and Contingency Plans

There is no way to assure perfect operation of all mission critical systems throughout the Year 2000 transition. The risk of system malfunctions and their damaging effects can be minimized if careful attention is paid to system and system-of-system (systems integration) testing, emergency response teams and operational contingency planning.

1. Testing

Inadequate attention is being paid to testing. Traditionally, half the cost and time of software development and repair are consumed in testing. Testing is critical not only for individual systems but for interface and "system-of-systems" operational assurance. For example, an end-to-end test of those systems needed to support a conventional cruise missile strike would incorporate related intelligence collection, analysis and processing systems, C^3 systems at many command levels, mission planning systems and several weapons platform systems.

Thorough system, and system-of-systems testing is essential to validate Year 2000 system renovation. System testing for Y2K compliance verification is the most difficult part of the renovation, validation and implementation process (and is often under resourced) for many reasons:

- Although the DOD, "Year 2000 Management Plan," Version 2.0, (still in draft at the time of this report) contains a comprehensive listing of Year 2000 critical dates, there are no standard test routines approved for widespread use. The USSOCOM Year 2000 Draft Test Plan, however, does contain checklists for known critical Year 2000 conditions.

- The great diversity of system functions (logistics, finance and accounting, communications, weapons systems control, intelligence), the variety of system configurations in widely deployed networks, and the large number of Year 2000-related fault possibilities, mean that no single test for Y2K compliance is feasible. Year 2000 problems may exist in software, firmware, hardware system functions, or on date

microchips embedded in control devices.

- Year 2000 system fixes can induce other faults in systems that can affect functions unrelated to the intended fix. A comprehensive Year 2000 test plan must exercise all system features to assure that the system operates as intended. Y2K faults may cause the system to crash or may give subtly incorrect answers; tests must detect both types of faults.

- Because of the promulgation of fixes, regression testing, both within and between, systems will become a major Y2K test effort, and must simulate many dates before and after January 1, 2000.

- Most critical systems interact with other systems. Even though each system checks out individually, system-to-system interfaces may not work. Several approaches exist to fixing Y2K system problems; systems renovated in different ways may not inter-operate. Although memoranda of understanding defining interface specifications between the owners and operators of interacting systems reduce the likelihood of system-to-system incompatibilities, the fact that system renovations are performed by a variety of contractor and vendor personnel leaves room for misinterpretations. Without full system and system-of-systems environment tests, there is no assurance of overall Y2K compliance.

- The system test plan and environment for Y2K compliance can be as complex as the system or combination of systems being tested. Test environments must be developed as systems are being renovated in order that tests are not delayed or rendered ineffective by poorly conceived test conditions.

- System tests must include operation with legacy databases to assure both proper system operation and the preservation of database integrity.

- Vendor Y2K compliance claims are frequently in error or incomplete. DOD must verify Y2K compliance for itself.

- Lessons learned from systems test experience on large, complex, interactive systems such as the Defense Messaging System (DMS) show that each time changes are made to individual system elements, the entire system or system-of-systems must be revalidated to assure overall system functionality.

- There is no central authority for certifying system Y2K compliance. At

present, when testing is performed by an independent agency, test results are forwarded to program managers or system operators who individually certify Y2K compliance. The agency itself cannot make that determination.

- The "take-it-out-of-hide" funding approach to achieving Y2K compliance virtually assures that testing is insufficiently planned and executed in many systems.

Ideally, mission-critical system and system-of systems validation testing would be carried out by independent agencies such as the Joint Interoperability Test Center (JITC), Defense Communications Test Facility (DCTF), DISA-Westhem or their Service equivalents. These organizations have expanded their capabilities to perform Year 2000 testing, however the large amount of complex testing that must be carried out on mission critical systems, the short time remaining, and the testing resources available, dictate that most Year 2000 testing be delegated to system owners with independent agency oversight. Authority for Year 2000 compliance certification, or certification review, should be vested in duly constituted certifying authorities such as JITC, DCTF, Westhem or their Service counterparts.

Since independent test agencies do not have their own funds to perform Y2K testing or testing technical assistance, system owners must pay for agency support out of current operating budgets. This is a significant disincentive to using the most competent system testing centers in DOD which are outside the control of the component. Independent testing centers (such as JITC, DCTF and Westhem) must be funded to conduct/assist with Y2K compliance testing or audit certification plans and results of most critical systems and other mission critical systems that do not have owners.

System (and system-of-systems) testers must be prepared to provide information on which to base claims for Y2K compliance. System characteristics and testing details and documentation should be carefully reviewed before a certification decision can be made.

Year 2000 test verification of a system or system-of-systems Year 2000 certification can be ranked according to risk of system problems in four levels (in order of least risky to riskiest):

Level 1: Certification by an independent Agency (JITC, DCTF, Westhem or Service equivalents)

Level 2: Certification by in-house authority such as the Program Manager, System Owner or Operator

Level 3: Vendor certification

Level 4: No certification

Currently there are few Level 1 systems

In view of the critical importance of testing in assuring proper operation of mission-critical systems and system-of-systems, all mission-critical systems should reach Level 1 or 2 status by the end of 1998. Those deemed most critical by the Joint Chiefs of Staff (nuclear weapons command and control, conventional global command and control, and mission planning systems, for instance) should receive Level 1 certification.

A standard set of planned tests such as those described in the USSOCOM Year 2000 Test Plan[1], as applicable to the subject system, should be mandatory for all certification testing.

2. Emergency Response Teams

Even in the most optimistic estimates of Year 2000 system operations, unanticipated problems will occur on many dates[2] before and after the January 1, 2000. Many of these problems will be minor but some major system failures can be expected. DOD's response to these problems should be in place before the end of 1998 to assure rapid restoration of proper operation.

System operators must be alert to the possibility of Y2K problems. When encountered, response to these problems should be graduated:

- System operators should be the first line of defense. Simple problems should be dealt with immediately by those in control of system operations in real time. These are the people most able to respond to unexpected problems quickly and should be trained to look for Y2K problems.

- System owners or program managers should establish a second echelon of emergency response to Y2K problems consisting of the technical staffs responsible for maintaining the system. These staffs are the subject matter experts in the operation of the specific system or system-of-systems that should be able to quickly comprehend where the problem has occurred.

- The Service System commands should provide backup capability for

[1] U.S. Special Operations Command (USSOCOM) Year 2000 Test Plan Draft of 12/17/97

[2] See the Year 2000 Management Plan, Version 2.0, draft, January 1998

system owners. The System commands have unique expertise in the operation of system-of-systems.

- The independent testing agencies (JITC, DCTF, Westhem and their Service counterparts) are tasked with emergency response to system problems as part of their mission and have emergency response capabilities. These experts should be DOD's resource for contending with the most serious Year 2000 system problems. These agencies should have emergency response teams available to step in quickly to resolve the most difficult system problems when they occur.

Emergency response plans are not yet in place at any of these four levels. Since the earliest anticipated problem dates occur late in 1998, DOD should now insist that plans for emergency response capabilities at the system operations and owner levels be developed for each system deemed mission critical. Additionally, the independent testing agencies need to develop rapid response capabilities for dealing with the most serious Year 2000 problems.

Triage procedures for managing responses to Year 2000 problems should be developed at the level to assure best use of emergency response capabilities.

Information on how to call in appropriate response teams to deal with system problems should be readily available to managers and operators of mission critical systems.

3. Contingency Plans

Mission critical systems must have contingency plans mitigating the risks of system malfunction due to Y2K problems. Such plans might include fast systems fixes (e.g., 28 year clock decrement) find out more about this and correct accordingly, operational work-arounds, engineering support, and manual backup or older system alternatives in case of system failure. The DSB Y2K Task Force notes that some system owners have already developed and put in place sensible plans to mitigate the effects of system failure; others, however, have yet to devise such action plans. Of particular concern are those system managers who plan to replace existing non-compliant systems with new hardware and software before January 1, 2000. Many of these managers have no plan for what to do if the planned replacement systems do not materialize in time.

Risk assessment and contingency plans must address such possibilities as:

- System crashes due to date failure

- Incorrect results due to errors in date data transmission and computation

- Impact on systems coupled with the contingent system

- Program crashes due to sending or receiving incorrect data or data fields

- Corruption of data due to incorrect data introduced into archives or destruction of data bases due to erroneous data cleansing

Contingency plans should address response times and provide a basis for prioritizing responses to problems.

The single manager of Y2K issues should require contingency plans of all mission critical system owners covering how system functions can be maintained in the event of system failure due to Y2K problems or failure of replacement systems to come on line in time to avoid Year 2000 effects. These plans should be accepted and understood by the operational community. The Unified Command should have a major role in judging the sufficiency of the contingency plans.

4. Summary

a. There has been inadequate attention given to the testing area.

This is very serious given that traditionally half the cost and time for software programs are consumed in the testing phase. Testing is critical not only for individual systems but for interface and "system-of-systems." For example: an end-to-end test of those systems needed to support a conventional cruise missile strike would test: relevant intelligence collection; analysis and processing systems; C^3 systems at many command levels; mission planning systems; and several weapon platform systems.

b. Other key observations relating to testing are:

- With the great range of DOD system characteristics and the multiplicity of potential Y2K problems, no single test will suffice to assure Y2K compliance.

- Testing is not an "after the fact" event. Test conditions and the test environment must be developed at the same time that system fixes are being made so that the test capability is ready when the system is remediated. This requires test personnel involvement throughout the five stages of Y2K system correction.

- Y2K certification through testing can be considered in four categories (in order of system assurance, highest first):

    1) Certification by testing by an independent agency

2) Certification by system owner in-house testing

3) Certification by vendor

4) No certification

- Ideally, DOD mission critical systems should all fall in Category 1. At the least, they should have category 2 assurance.

- Independent testing agencies within DOD (e.g., JITC) are alarmed at the lack of requests for Y2K testing assistance by system owners and operators. Since their support is funded by customer funds, it is likely that the "take-it-out-of-hide" policy has resulted in delayed test activity which will likely snowball as Y2K critical dates approach.

- DOD has no central certification authority. Although the Y2K management program describes test conditions, there is no assurance that the conditions are being uniformly applied. Those independent agencies within DOD that perform, oversee or assist with Y2K testing are prevented by policy from "certifying" Y2K compliance. Instead the results of their tests are forwarded to the system owner who makes the compliance determination.

- Contingency planning for unanticipated problems is not being uniformly pursued.

No one is taking steps to plan for and implement Emergency Response Teams [ERTs]. Several organizations in DOD have provision of emergency response teams as part of their missions. These organizations have not yet begun to plan for the emergency response requirements presented by Y2K problems.

D. Business-like Systems

Discussions were held with the Principal Assistant Deputy Under Secretary of Logistics, members of his staff, and various major weapon systems to gain insight on business-like systems — Logistics, Transportation, and Financial Operations. All of these business-like systems are heavily date-dependent and are extensively impacted by Y2K. This could pose a serious threat to the ability of DOD to carry out its mission. There are enterprise-wide systems (i.e., Defense Logistics Agency [DLA] and Defense Financial and Accounting Service [DFAS]), and each branch of the DOD has its own systems. These systems have been significantly automated and in many cases can not fall back on manual processes. It is critical that these systems be corrected well before the Year 2000, and that a coordinated test plan be implemented.

1. Logistics

In the field of logistics, most systems are very complex. They are also highly customized and integrated. Weapon system operations are critically dependent on timely provisioning of supplies and equipment. In order for provisions to arrive in a timely fashion, scheduling and long lead-times are often required. Because of the nature of logistics, information systems supporting logistics are heavily date dependent. For these reasons, immediate corrections are required, and manual work-arounds are not possible. Due to the highly customized nature of logistics information systems, few, if any, COTS replacement systems are available. A further complication is the fact that many of the critical systems and operations supporting logistics are handled by suppliers that are not organic to the unit being supplied. This, in turn, increases the difficulty in carrying out interoperability testing. These technical and organizational Y2K problems are further exacerbated by the fact that the DOD has been traditionally slow in providing direction to suppliers.

2. Transportation

Transportation is integral to an efficient logistics system, and is key to the basic operation, maintenance, and support of weapon systems. It is also internal to overall logistics support processes and systems. While many transportation systems are date dependent, in contrast to logistics systems, they are also quite similar to commercially available systems. For this reason, use of COTS systems or commercially available services may help alleviate some of the problems associated with Y2K.

3. Financial Operations

Financial operations by their nature are heavily date dependent, and are highly integrated into networks of systems with other financial institutions. Financial systems are also more vulnerable to a system shutdown. Supplier data feeds are impacted at EDI interfaces. Problems stemming from financial operations systems failure would also have a major impact on managing suppliers. Many DOD suppliers could not tolerate long-term cash flow problems caused by system failure, because of the supplier's small size and relative dependence on DOD contracts. However, some systems could operate manually for a short period. Many COTS systems and consulting services are available that could quickly be implemented in case of an emergency.

E. Operational Systems

The Operational Systems group examined three categories of systems for Y2K problems: weapon systems, command, control, and communications (C^3), and Commander-in-Chiefs (CINCs) concerns.

1. Weapon Systems

Briefings were provided to the task force by four major weapon systems organizations including AEGIS, F-15, MLRS and PATRIOT. Additional briefings were provided which related in part to interfaces to weapon systems (e.g., E-6B, AWACS, JCS/J6 Nuclear Weapon Interfaces, etc.).

The four major weapon systems had some important characteristics in common relative to Y2K:

- All had program management organizations in place with the clear ability to identify and respond to issues as they were identified.
- All had adequate resources to deal with any problems which might arise.
- All had programs on-going to identify and solve possible problems.
- Although time oriented, none of the weapons systems were calendar oriented so there was little concern as to whether they would work when needed.
- There was relatively little concern about the ability of the systems to meet mission requirements except with regard to interfaces to supporting systems such as mission planning, C^3I, training and logistics. For example, in the case of the F-15, there is a clear dependency on the Mission Planning System functionality if the F-15 is to carry out its strike mission. The F-15 SPO is very aware of this situation and is actively involved with the correction of Mission Planning System deficiencies. Also, the significance of operational interfaces for systems beyond the control of PATRIOT systems organization was noted as an uncertainty. This type of uncertainty was also noted for some of the other weapon systems.

It is evident that the major weapon systems managers are fully aware of the Y2K issue and are actively looking for problems and solutions. There is not much concern that they will experience ugly surprises, mature programs with veteran program management organizations have incorporated Y2K into the normal development and upgrade process. However, there is room for the major weapon systems managers to look harder at the supporting systems (e.g. training, logistics, C^3I, etc.) upon which their systems rely.

In addition, there is little evidence of any management, planning or resources in place for large scale joint interoperability demonstration testing as would be required to resolve the uncertainties in the significance of operational interfaces beyond the control of the weapon systems managers.

Contingency planning is not in place for testing or for the solution of late breaking surprise problems. This lack of contingency planning is somewhat surprising since major weapon systems managers are known for not leaving much to chance.

However, of all of the areas the Y2K panel has examined, we believe that the major weapon systems per se are in the best shape, both to avoid Y2K problems, and to address them should they arise.

2. Command, Control and Communications (C^3)

The task force received briefings and/or participated in Y2K discussions with C^3 personnel from Defense Information Systems Agency (DISA), Joint Chiefs of Staff (JCS/ J6), OPNAV (N6), Head Quarters Marine Corp (HQMC) (C^4I), Air Force Program Executive Office (AFPEO/ C^3), Airborne Warning and Control System (AWACS), Assistant Secretary of Defense (ASD C^3I), Joint Tactical Information Distribution System (JTIDS) and the E6-B program.

Important characteristics regarding Y2K, and common to at least two or three of these organizations dealing with C^3 issues include:

a. All have strong program management organizations in place with senior executive visibility and the clear ability to identify and respond to issues as they are identified.

b. All have programs on-going to identify and solve possible Y2K problems.

c. All believe they were basically on schedule for systems under their authority and responsibility. For example, AWACS and JTIDS expressed that their systems are well in hand. However, almost all expressed concern regarding interfaces and interoperability particularly for systems not under their control but critical to their missions. These concerns included known and unanticipated Y2K problems. Several organizations noted the difficulty in obtaining status information on Y2K activities for many of these systems. The DIST was inadequate in this regard not only for systems in DIST but also because intelligence systems (e.g. NSA, etc.) are not in DIST and not reported on elsewhere. The DIST was also regarded as user unfriendly.

d. The management of Y2K varies significantly across organizations. Mature programs in veteran program management organizations have adopted management processes and metrics expected from such organizations (e.g., AWACS, JTIDS, E6-B, etc.). Management of newer programs lacked the strong processes and metrics to provide confidence

in assessing progress on Y2K issues. For example, this was evident even with such mission critical systems as GCCS and GCSS.

e. Several organizations noted significant dependence on COTS hardware and software products and expressed the need for a Y2K compliant infrastructure or a central COTS product test agency to provide the DOD with a single central source of valid Y2K compliance information on COTS hardware and software products.

f. Almost all expressed the beneficial aspect of the Y2K problem as an opportunity to terminate ineffective legacy systems and replace them with more effective Y2K compliant systems including new systems if the budget resources and funding flexibility happened to be available. Several expressed concern regarding OMB statements regarding the possibility of directing Federal departments to delay IT modernization efforts in order to fix Y2K problems if this meant that key modernization efforts underway which not only provided improved and needed functionality but also fixed Y2K problems became possible targets for delays.

g. Several expressed significant concern regarding recruiting and retaining the skilled IT civilian and military personnel needed in the DOD to address the Y2K problems during the next several years, the most critical time period. It was clear to all that there is an IT employment environment with significant commercial demand, a national shortage of skilled personnel and escalating compensation packages. This exists in the face of the recently announced Defense Reform Initiative (DRI). The continued efforts to downsize the DOD, with the elimination of existing careers in military and civilian personnel IT and the DOD initiatives to outsource various IT functions exasperate the problem.

h. All understood the criticality of achieving Y2K compliance for mission critical C^3 systems and how broadly these systems can affect DOD operations. In fact, C^3 systems represent about half of the warfighters top 20 Y2K concerns for the CINCs.

i. Several organizations recognized and were working significant Y2K issues concerning non-compliant telephone switches. Of the 663 DOD switches worldwide, about 33 percent are not compliant and most of these are NORTEL products. Some concern existed regarding the availability of replacement switches given the commercial demand in "fixing" Y2K switch problems. Several organizations also recognized and were working significant Y2K issues concerning non-compliant Personal Computers (PCs) needing replacement, MUX-IDNX non-compliance and U.S. Message Text Format (MTF) problems.

j. Many expressed concerns regarding the "take-it-out-of-hide" approach to fund all Y2K fixes. They admitted the fact that although well-funded development programs had funds to fix Y2K problems, other programs were at the stage of not having funds identified, and were "hoping" funds would be made available to fix their Y2K problems. It was clear that funding flexibility (e.g., ability to transfer funds) was an issue inhibiting timely action by some organizations to fix Y2K problems. Finally, highly structured processes such as those required for MAISRC programs have inhibited timely action on Y2K issues. Attention to having such processes modified to allow critical Y2K issues to be addressed in a more timely manner is important.

Beyond those items mentioned above, clearly more attention should be given to large scale joint interoperability testing. "Test early and test often" is a recommended theme. Field testing of C^3I systems in controlled environments is particularly important to address interfaces and interoperability. C^3I interfaces remain a critical potential Y2K vulnerability particularly with decentralized system responsibilities. Also, problems observed in early tests should not be condemned as was unfortunately the case by the press with the JWID `97 GCCS tests. Such actions discourage organizations from testing early to understand their Y2K problems in order to have sufficient time to fix problems observed.

Additional attention also is important for development of contingency plans and for the formation and exercise of Emergency Response Teams (ERTs). All Y2K problems will not be solved and tested. There will be surprises and many unknowns. Appropriate planning for such contingencies is critical.

The human resource problem appears to need high level attention. As time passes, Y2K issues will increase in their importance and skilled DOD staff is critical. Y2K consideration should become factors in the DRI, downsizing and outsourcing decisions. Special incentive programs are important to consider. Strong teaming with industry is recommended to reduce the vulnerability to staffing issues.

Finally, it is important to have special Y2K funds available for programs not currently well funded, for interoperability and interface testing and for surprises. In addition, increased funding flexibility and the reduction of process and procedural barriers are important to consider to allow critical Y2K issues to be addressed in a timely manner as they arise.

3. Commander-in-Chiefs (CINCs)

The task force received briefings from and participated in discussions with Y2K organizations from two CINCs, USSTRATCOM and USACOM. In addition, briefings by JCS (J6) and E-6B personnel provided a broader perspective regarding CINC activities on Y2K including possible implications for nuclear systems.

The CINC organizations had some important characteristics in common relative to Y2K:

a. Both have strong program management organizations in place with the clear ability to identify and respond to issues as they were identified.

b. Both have programs on-going to identify and solve possible problems.

c. Both noted the strong dependence on the Services and external agencies for achieving Y2K compliance for the weapon systems, the intelligence systems, the facilities, the C^3 systems and other systems critical to CINC missions. They also noted the difficulty in obtaining status information on Y2K activities for many of these systems. The DIST was inadequate in this regard not only for systems in DIST but also because intelligence systems (e.g., NSA, etc.) are not in DIST and not reported on elsewhere.

d. Both expressed concerns regarding interfaces and interoperability particularly for systems not under their control but critical to their missions. These concerns included known and unanticipated Y2K problems.

e. Both are dependent on significant COTS hardware and software products and noted the need for a Y2K compliant infrastructure or a central COTS product test agency to provide the CINCs and the rest of the DOD with a single central source of valid Y2K compliance information on COTS products.

f. Both participate in the CINC Y2K sessions which produced the consensus Top 20 list of mission critical systems for the warfighters which is currently being staffed for approval. Greatest concern was expressed regarding C^3 systems such as the DII COE, GCCS, GCSS, DSN, Red Switch Network, DMS, and DISN.

g. Both believe they are on schedule for systems under their responsibility.

USSTRATCOM activities focus on 113 mission critical systems including 88 for strategic war planning, 11 for command and control, and 14 for command management. Systems are in the renovation/validation phase or are planned for decommissioning. Y2K activities are facilitated by the major on-going modernization efforts. USACOM indicated that all of their mission critical systems are the responsibility of other organizations.

Nuclear system interfaces, war planning, and C^3 were discussed with USSTRATCOM, JCS (J6), and E6-B personnel. These systems are receiving appropriate and strong attention in the U.S. and significant progress is evident. However, several areas were noted for increased attention. One was Y2K interface and interoperability testing. Although C2 testing and communications testing are

progressing separately, it is important to have more comprehensive C^3I testing in an integrated fashion. Another area was NATO and other allies. Clearly, other countries are behind the U.S. in addressing Y2K issues.

There was no evidence that DOD was taking strong, positive steps to increase awareness of Y2K issues with our defense partners to assure appropriate actions toward Y2K compliance, particularly for NATO nuclear systems. Finally, concern was expressed regarding other countries with nuclear weapons such as Russia and China and their actions or, more importantly, perceived inaction regarding Y2K issues. Clearly, it is in our national interest to have positive command and control as well as safety and physical security for weapons of mass destruction in Russia and China, particularly nuclear weapons. DOD has not been pro-active in Y2K education and awareness effort for these countries.

Y2K issues for the base infrastructure were discussed with the above organizations as well as others. Y2K issues include basic utilities (e.g., electrical power, telecommunications, water treatment, sewage, etc.) as well as embedded software in microprocessors in equipment such as elevators, heating and air conditioning systems, security systems, and other systems critical to normal base operations. Although it was noted that the base infrastructure is the responsibility of the Services, it also was noted that most Y2K efforts in this area appear to have started later than the basic computer hardware and software efforts on Y2K. This is also true in the commercial environment. Increased attention in this area by the DOD is warranted.

Foreign bases were of particular concern, again because most other countries are behind the U.S. in addressing Y2K issues. Yet, these bases are dependent to a large degree on local utilities such as electrical power and telecommunications. Increased attention to foreign bases by the DOD is warranted including contingency planning for Y2K problems in the host country. Also, DOD needs to assist our military and coalition partners in addressing their Y2K problems, to ensure continued capabilities before and after January 1, 2000.

CINC IT budgets are small. Increased funding flexibility and a source for additional resources are needed to address Y2K issues, particularly to achieve adequate interface and interoperability testing. Such testing is critical for CY98. In one case, testing is being postponed to wait until systems not under a CINC's responsibility are deemed Y2K compliant. "Systems of systems" tests are recommended such as a conventional cruise missile strike scenario. Such a Y2K test scenario would test intelligence collection, analysis and processing systems, C^3 systems at many command levels, mission planning systems, and weapon platforms. Systems tested in such a scenario span many organizational responsibilities but all support the warfighter.

Clearly the CINCs are aware of Y2K issues and are addressing them vigorously for systems under their responsibility. However, they are in the position of being heavily dependent on the Y2K activities by the Services and agencies in order to meet their mission requirements.

F. Intelligence and Information Warfare

1. Information Warfare (IW) related to Y2K

The DSB Year 2000 Task Force had briefings from Booze, Allen, and Hamilton on Information Warfare (IW), and had briefings and discussions with the National Security Agency (NSA), the National Reconnaissance Office (NRO), the Defense Intelligence Agency (DIA), the National Imagery and Mapping Agency (NIMA), and the Community Management Staff (CMS) of the Director of Central Intelligence (DCI), and their support contractors.

In addition, we have had overviews from various operating functions from within the DOD which raised IW concerns and issues. Based upon the information presented to date and conversations with task force members, the team has identified the following action items with regard to information warfare concerns.

There are a number of areas of concern relating to the impact of Y2K on intelligence and information warfare. In attempting to fix the problem, Y2K "fixes" will result in patches on patches, that is, a fix on one system may require a fix on another to enable the systems to interface, etc. Also, all fixes have a fixed date cliff in that they have to be fully implemented and tested by December 31, 1999. The significant time compression of work required to have everything done on time is bound to result in unexpected errors. As a result, testing will be also be shortchanged, as insufficient time will remain to carry out needed testing of system fixes. In an effort to meet the time constraints imposed by the date cliff, out of country coding expertise may be used which could increase vulnerabilities from remediation efforts. This could result in some increased threat from global hackers, as foreign coders could not be held to the level of security checks of U.S. coders. In general, the Y2K remediation community is not thinking in terms of IW threat.

A number of actions need to be taken to mitigate the impact of Y2K of the intelligence and information warfare threat. Organizations should establish contingency plans to implement work arounds of Y2K issues. The United States has "bet the farm" in the sense that we are sizing our force structure predicated on information superiority, and this is known to our adversaries. They may well intend to attack our command and control systems (our information dominance) to give them an asymmetrical response to our "technical superiority." They should begin by determining the most critical of DOD systems that could be affected. To ensure objectivity, renovation work on absolutely critical systems needs to be independently verified. The verification process should include very selective negative testing as

well as positive testing to see that new functionality has not been inserted with the remediated code

Because System Administrators (SAs) are the first line of defense during the period spanning the Y2K transition, DOD should take steps to improve their effectiveness. DOD should elevate the role of System Administrators, and provide adequate training, security clearances and back ups. System Administrators should also be brought into the remediation planning process. In addition, DOD should solicit SA views about techniques to detect Y2K problems in real time, and courses of action that could be taken on how to respond. As noted previously, independent validation of implemented changes needs to be conducted as does strict configuration control. To mitigate IW threats, changes made to critical software should not be advertised, and Y2K fixes and problems should keep a low profile on the Web pages. Unclassified DOD systems should be examined to determine if they have the capability to provide bad data to classified systems. System Administrators also need to take active measures to raise protective barriers. Such measures should include the installation of effective firewalls, the use of dynamic passwords, and sophisticated filters and encryption where possible. These recommendations are based on the following observations and issues.

2. Information Warfare Threat

It is highly likely that DOD information systems will be probed or penetrated by hackers coincident with the Year 2000. An abundance of information relating to Y2K problems and the "fixes" to those problems is increasingly available on the web and other public sources. Hackers from many parts of the United States and the rest of the world undoubtedly will share information about Y2K weaknesses in computer systems. In some cases "communities of hackers" may act in concert to demonstrate their ability to cause mischief. While the likely focus of such efforts will be information systems in the private sector, the DOD also is clearly an attractive target. We should expect that hackers will expose and widely disseminate vulnerabilities to Y2K solutions.

Increased vigilance by system administrators will be very important during the period spanning the Y2K transition. The Y2K transition will not be a discrete event centered on December 31, 1999; rather, the transition will span a number of months after or perhaps years as a wide variety of systems are remediated to accommodate four digit year data. Thus, the period of increased DOD vulnerability is surely to be lengthy as systems not initially identified as "mission critical" are remediated after 1 January 2000. The likelihood of successful penetrations during these periods dictates that each MC system have a contingency plan for successful mission accomplishment to "work around" Y2K issues.

While perhaps less likely, there is a substantially greater area of concern. That relates to thoroughly planned, intentional activities by a foreign power,

transnational group or terrorist group to use DOD's remediation planning and execution period to install malicious code in systems critical to the effective functioning of the DOD! Consider that thousands of computer programmers and engineers have been brought relatively quickly into remediation efforts for thousands of DOD essential systems. Corrupting very, very few of these systems could have dramatic impact. Furthermore, COTS by the thousands of applications reside in DOD systems and while most COTS operating systems software is developed in the U.S.; much other software (such as device drivers and applications) is developed on foreign shores. Programmers in India, Russia, China, Israel and Ireland are all involved in off shore code development. Many of the telephone switches in the U.S. come from foreign sources, and, as we know, 95 percent of all DOD communications ride on our public switched networks!

However, not all of our most likely adversaries will be foreign. Given all of the downsizing and centralization activities in the U.S. and the DOD, it is quite possible that disaffected citizens with strong technical skills and a dislike for their former organization could work to cause damage and disruption in computer systems, or sell their skills to terrorists, drug or crime cartels.

3. Phase by Phase Threat Analysis

How might our adversaries plan to conduct an IW or Information Operations attack against our Y2K Conversion Model?

During the Assessment Phase: an adversary might try to influence the Assessment by falsifying Y2K vulnerability analyses, by identifying critical systems upon which to focus malevolent actions (targeting), by influencing contingency plans in the least effective direction, and by trying to have resources misappropriated or misdirected.

During the Renovation Phase: insert malicious code; convert, replace or eliminate databases; insert triggers, Trojan horses or logic bombs; or work to alter the focus of software upgrades and remediation in the least effective direction. Install holes in key systems to allow "data mining" or intelligence gathering over an extended period of time. (Consider JCS Exercise Eligible Receiver 97 in PACOM.)

During the Validation Phase: refine attack plans and implants; falsify validation data; provide or sell bad test equipment, tools or procedures.

During the Implementation Phase an adversary would attempt to prepare for or execute an attack, possibly stimulated by world or political events outside the U.S. Department of Defense.

4. Counter measures

Possible counter measures, which may thwart or at least mitigate these kinds of efforts, include the following:

- Determine the real criticality of DOD systems and developing and reviewing contingency plans.

- Independently verify renovation work for those systems that are absolutely critical. This might include very selective "negative testing" as well as "positive testing." That is, testing to insure that new functionality has not been inserted with the remediated code. Positive testing, verifies only that the year digit issue is fixed.

- For absolutely critical systems, internally verify portions of the validation process. Use the two person rule.

- Independently validate and verify (IV & V) implementation changes.

- Conduct strict configuration control which will make it easier for us to understand our security posture coincident with remediation.

- Do not advertise changes made to critical software. Keep a low profile on the Web pages.

- Look at unclassified DOD systems to determine if they have the capability to provide bad data to classified systems thereby inhibiting mission execution. Candidate systems include logistics, weather, finance, medical and so forth.

It is important that the Defense Department create capabilities to function in reduced mode operations. Therefore, it is desirable that a systems of alerts and responses be adopted which will help the JCS, the CINCs and other key elements of the DOD respond adaptively to degradation's in its systems.

Below is a table (originally proposed in the 1996 DSB Study on Information Warfare - Defense) summarizing threat conditions and possible responses based on a perimeter defense. This concept is for systems, analogous to the DEFCON Conditions used for so many years in the DOD regarding military readiness.

CONDITION	SITUATION	REQUIRED RESPONSE
I. Normal	• Normal threat-crime/ incompetents • Normal activities in all sectors	• Normal actions and requirements
II. Perturbation	• 10 percent increase in incident reports, regional or functionally based • 15 percent increase in all incidents	• Increase incident monitoring • Look for patterns across wide range of variables • Alert all agencies to increase awareness activities • Begin selective monitoring of critical element
III. Heightened Defense Posture	• 20 percent increase in all incident reports • Condition II with special contexts	• Disconnect all unnecessary connections • Turn on real-time audit for critical systems • Begin mandatory reporting to central control
IV. Serious	• Major regional of functional events that seriously undermine U.S. Interests • Condition II/ III with special contexts	• Implement alternate routing • Limit connectivity to minimal states • Begin "aggressive" forensic investigations
V. Brink of War	• Widespread incidents that undermine U.S. ability to function • Condition III/ IV with special contexts	• Disconnect critical elements from public infrastructure • Implement WARM protocols • Declare state of emergency

Table 2 — Threat Condition/ Response

Beyond the turn of the century there are real concerns. It is certain that all remediation will not have been accomplished by the year 2000. Furthermore, there probably is a greater chance of software penetration later due to exposure during the Y2K correction processes.

5. Intelligence Summary

What we regularly refer to as the Intelligence Community, is actually a confederation of activities and agencies who singly and collectively have responsibilities for intelligence activities on behalf of the United States. Thus, the Director of Central Intelligence (DCI) does not have line authority over each of the elements of the "Intelligence Community" in the same sense that the Secretary of

Defense has authority over elements and agencies of the Department of Defense. From the perspective of Y2K, this means that the Intelligence Community Management Staff (CMS), under the DCI is chairing a collaborative effort within the community regarding remediation efforts in support of Y2K. For example, while the Defense Intelligence Agency (DIA), the National Security Agency (NSA), and the National Imagery and Mapping Agency (NIMA) are responsive to the CMS direction regarding the reporting and evaluation of Y2K remediation activities, each of these organizations is an independent Defense Agency under the SECDEF.

The IC wrestles with the same issues as does ASD(C3I) regarding Y2K: no additional funding, take-it-out-of-hide; "Centralized" direction with decentralized execution and remediation; a large number of systems designated as mission critical; stressful deadlines for testing and integration; January 1, 2000 applies to all systems; large numbers of legacy systems, a number undoubtedly with poor documentation; ongoing programs are better able to allocate resources (funds) to remediation than are programs whose systems no longer are in development.

There simultaneously are additional stresses on the Intelligence Community:

- Very large archived data bases.

- Some difficulty in understanding "all of the interfaces" driven by intelligence data. That is Intelligence Agencies "broadcast" information to hundreds, in some cases thousands, of consumers and may not be aware of the uses to which recipients put the intelligence information. Intelligence data rarely are "hard wired" as interfaces to operational systems. Thus, testing of these "interfaces" is often difficult or in some cases practically impossible.

- Information of potential adversary geographic locations provided by Intelligence Sensors often drive threat warning algorithms in operations systems, and only the sponsors of the operational system will know the extent to which this occurs.

- Testing of Intelligence Systems offer some unique challenges, such as testing of interfaces of existing space based sensors which potentially will be effected by remediation efforts. If you "lock up a satellite" during such a test, how do you recover? With regard to the planning of testing, the Intelligence Community has the same approach as DOD, in that each activity is responsible for scheduling and conducting (or causing to be conducted) its own testing. Thus, we note that NIMA is creating a Testing Master Plan, much in the same vein as USSOCOM. DIA is considering a special Y2K test facility, and also plans to use the Joint Integration Test Facility (JITF) at Rome, New York. Both NSA and the NRO consider testing to be the responsibility of the applicable program manager. It is

clear that the Intelligence Community could benefit from some of the suggestions and structured approaches proposed for above.

Members of this DSB Task Force met with and discussed Y2K issues on several occasions with members of the CMS and Intelligence Community. The good news is that Seniors, that is Agency Directors, in the Intelligence Community are alert to and placing significant emphasis on Y2K remediation. In each of these agencies, either the CIO, or a Y2K Task Force, or both, are charged with responding to Y2K problems. As in the case of the DOD, the intelligence community has chosen to respond, or remediate, through program managers or Program Element Officers of existing programs.

Reporting of Intelligence Community Y2K planning and remediation activities are, because of classification, not included in the DIST; thus most of OSD does not know the status of planning for and execution of Y2K remediation. Therefore, there is some uneasiness about whether Intelligence will be available when and where needed. Although a system of accounting and reporting is in place within the Intelligence Community analogous to the DIST used by DOD, there needs to be a more direct and clear linkage between DOD and the Intelligence Community Y2K planning and execution efforts.

There are other similarities to the DOD. A major similarity is the apparent difficulty in identifying REALLY "mission critical systems". In response to the original guidance from OSD soliciting identification of mission critical systems, the Intelligence Community initially identified over 2,200 "mission critical systems". As OSD began to narrow the criteria for "mission critical" the numbers of IC mission critical systems began to decline. For example, NSA, which identified the largest numbers of such systems started out with over 2,000 reported systems, reduced that to 744 in December, then to 456 as of January 31st.

Each of these reductions was the result of refining the definition of what constituted REALLY critical systems. In this vein, the Command and Control community of DOD has identified 20 key systems in the intelligence community that are considered necessary for DOD minimum essential capabilities. It is not surprising that the Intelligence Community would consider a larger number of its systems to be mission critical, than the number of intelligence community systems the SECDEF would consider critical to DOD missions. This is so because the Intelligence Community supports all of our government, not just the DOD. Thus support to the other cabinet departments and agencies, as well as the National Security Council and the White House, are properly considered by the Intelligence Community as equally critical Y2K systems issues.

Since many intelligence community systems support several of these agencies and DOD at the same time, it would be a most difficult task to identify systems totally unique to DOD requirements. It might be misleading to attempt to do

so. As a side note, it is interesting that the DOD considers its financial systems to be mission critical, but that after OSD narrowed its definitions, NSA removed its financial system from its list of mission critical systems.

So how is the Intelligence Community doing? In the case of known problems, progress appears to be pretty good--at least from the reporting perspective.

- Very large archival data bases are known (there probably are not huge data bases that no one knows about) and have well established data dictionaries, thus remediation should be straightforward. The very size of these data bases, however, offer significant challenges to insure that "all" necessary changes have been made, AND TESTED!

- In at least one case, NIMA, an additional problem exists. A very large (read huge) archived imagery data base was designed with a "first-in, first-out" protocol. That is, imagery requires so many gigabytes of storage, the system was designed to "self purge" so that automatically several years of imagery would be archived to permit comparison of new imagery with former images of the same facility to detect change. Therefore, if a date were to be misread as being significantly wrong (at the 00 date boundary for example), the system might automatically purge all information prior to, or after, that date wiping out years of crucial data. This problem is important, it is known, and NIMA has its support contractor focusing on this issue.

- There is concern in parts of the intelligence community that THE Automatic Digital Network (AUTODIN) to DMS conversion offers risk as we approach the millennium. For example, the DMS components required to process classified information have not yet been let for contract to the developer. Both the DOD and the Intelligence Community must have either AUTODIN or DMS classified message processing. AUTODIN cannot be taken down without this capability resident in DMS. It is being "assumed" that this key development will proceed as scheduled. In this regard, the Intelligence Community finds itself in the same position as DOD in that failure of planned improvements, developments or remediation efforts can have a significant adverse impact for which good contingency plans are essential.

- NSA's addressing of crypto issues seems to be on everyone's' critical path. Areas of potential concern have included the Electronic Key Management System (EKMS), and the STU-III. NSA believes that both of these activities are on track. Development of EKMS is proceeding as scheduled.

With respect to the compliance status of the STU-III and its supporting

infrastructure, the full results of actual formal testing are not expected to be available until May 1998, which unfortunately reflects a slip from the original March date. At this time however, based on work done in NSA's STU-III program offices, and at their contractors facilities, NSA is confident that not only are the STU-III terminals, per se, not appearing to have any issues–the infrastructure supporting STUs looks like it is also in good shape based on extensive preliminary testing. The NSA Director of Information Security (DDI) is confident that the formal full-scale testing will be completed by early May. Additionally, the DDI reports that he is committed to having a completely tested and validated compliant system in place by December 31, 1998.

Although a number of the programs have conducted risk assessments and identified contingency plans--in some cases new systems are being accelerated to replace legacy systems--none of the intelligence agencies has created a "priority system" for determining what contingency plans are required. Close liaison with DOD is required to identify where the critical paths lie so that remediation and testing may be scheduled in such a way as to dovetail with DOD needs. Nowhere is this more true that regarding the issue of systems, and "system-of-systems-testing."

There are a couple of issues within the Intelligence Community which may well have parallels with the DOD community and its allies. Firstly, NSA has cooperative arrangements with over fifty nations. Although NSA has advised each of these nations that NSA has adopted a two digit windowing approach to the year field problem; each of the nations is responsible for its own remediation. Thus, it certainly is possible, if not likely, that one or more of these interfaces will experience problems between NSA and the 2nd or 3rd party nation with whom data is to be received or exchanged. "Testing" these interfaces in some cases may not occur until the problem shows up in operations.

Secondly, a number of NSA field and service cryptologic stations have over the years had "cottage industry" software systems and upgrades developed and installed for specific applications pertinent to the mission of that station. The extent of this "cottage industry " software is not well known by NSA and in some cases probably not even well understood by the station itself. Problems with this software may cause local problems for the field stations as the year 2000 rolls over. (The CINC's probably have similar problems resulting from decades of software and applications support local to each of the CINCs. These software packages are often poorly documented and may not necessarily be identified in the ongoing DOD reporting and remediation activities.)

In summary, the Intelligence Community faces many of the issues that confront DOD in general. There is a cogent need to identify truly mission critical systems. This must, at least in part, be accomplished in concert with ASD(C3I). From this should be created a prioritization of resources and contingency plans around those systems. Specific test plans should be created to insure that

interfaces to DOD mission critical systems will function. And, crisis action teams or emergency response teams must be created to support the Intelligence Community and interface with their defense counterparts. Finally, the Intelligence Community needs to share with ASD(C3I) and key DOD elements all data on Y2K plans and remediation.

G. Medical Systems

Discussions were held with the OASD(HA) Defense Medical Information Management (DMIM) organization. Clearly there is senior executive awareness of the Y2K issue in the DOD medical community and that strong efforts are underway to identify and solve Y2K problems. These Y2K efforts have been set in motion by the OASD(HA) in coordination with the Service Surgeon Generals representing strong direction from top leadership.

An Integrated Product Team (IPT) was formed during 1996 to address Y2K issues in the Military Health System (MHS). IPT membership represents each of seven business areas (clinical, executive information and decision support, logistics, resources, infrastructure, theater and other) as well as each military department. The IPT has identified 112 systems for which Y2K activities are being tracked. A November 1997 report indicates assessment is 100 percent complete, renovation 42 percent complete and validation 25 percent complete. The goal is to complete all phases, including implementation, by December 1998. Contingency planning is to be part of the MHSS Y2K Management Plan to be completed December 1997. A joint interoperability exercise is planned for January 1999.

Resources are believed adequate to address Y2K issues. Of the 112 systems being tracked, 43 have been assessed as compliant, 25 are designated to be replaced as part of normal modernization, 8 are to be retired and the Y2K specific funding is believed adequate to address the remaining 36 systems.

Biomedical devices are being addressed by a tri-service group with data maintained at Ft. Deterick. The Services have compiled inventories of biomedical devices in use, a very important step in assessing the situation. Information on biomedical devices is being shared with a similar group at the Department of Veterans Affairs. Industry responsiveness is evident and supported by FDA actions as well as the Medical Safe Practice Act.

Y2K readiness of facilities and utilities is the responsibility of the individual Services who manage each of the facilities. The OASD(HA) is requiring the Services to report Y2K status for facilities and utilities. The Services also are responsible for the locally procured PCs and other COTS hardware, software and utilities such as electrical power and telecommunications. Particular attention is important regarding the medical hospital and clinical facilities and supporting utilities in foreign countries because most foreign countries lag the U.S. in their attention to Y2K.

One of the more complex areas being addressed by the IPT is interfaces with systems in other functional areas such as personnel, finance and logistics. Although risk analyses on interfaces are being conducted, Memorandums of Understanding are in place and some testing is being done, more and broader testing at earlier times than currently planned is important, particularly during CY 1998. This includes "system-of-systems" testing. The Joint Warfare Interoperability Demonstrations (JWIDs) could be a logical time to further test Y2K, particularly cross-functional interfaces. For example, test scenarios of systems to support casualty evacuation or the provision of blood supplies would test personnel systems, medical systems, logistic systems, transportation systems, as well as C^3 systems at many command levels.

Overall, it is clear that Y2K issues in the medical area are receiving strong attention by OASD(HA) and the Services and appear to be further along than similar activities in the commercial community. The DOD should continue to support fully the OASD(HA) Y2K plans, facilitate cross-functional interface testing, and protect Y2K funding.

H. Summary Finding

The Y2K problem is a very serious one. It is a big system and system management problem. DOD is experienced and capable in analyzing, structuring and managing such programs.

Further, Y2K is a CEO problem, not just a CIO problem. It needs direction and guidance from the top. Its solution must involve all users of IT which certainly includes the Chairman, JCS, and the CINCs as well as the more traditional users.

III. Recommendations

The Task Force makes three major recommendations:

A. USD(A&T) should appoint a full time executive

The USD(A&T) should appoint a full time executive with the requisite authority and staff to provide the needed leadership and the overall plan for addressing the Y2K problems. The breadth of the Y2K problem, spanning as it does all aspects of military systems and operations, requires that OSD oversight of Y2K activities go well beyond the IT focus. Continued active involvement of the C^3I community is, of course, not to be lessened in any way as the result of this recommendation. Specific tasks to insure that each area is following a disciplined approach, is getting reliable support, and has reasonable consistency with the rest of the Department follow:

1. Identify the REALLY Mission Critical Systems

a. Work with components to determine and understand the consequences of failure to "fix" each "mission critical" system.

b. Work with the users to apply the "so what" test to determine those absolutely critical ones and establish a prioritized list.

2. Management

a. Require a milestone program plan for fixing these systems including identification of needed resources.

b. Reduce the number of meetings/ reports but insist on meaningful reports against a milestone program plan. Negotiate reasonable reporting requirements with OMB.

c. Develop special, streamlined procedures including funding flexibility to allow Program Managers the needed quick response capability warranted by Y2K problems.

3. Testing

NOTE: This area is, without question, most in need of direction.

a. Provide an outline of a testing approach and define results deemed adequate by OSD.

b. Provide for central certification authorities that can assure a uniform

approach to Y2K compliance by doing the testing themselves, by overseeing testing, by assisting with test design or by auditing test procedures.

c. Require for each program, system and "system-of-systems" a test plan which includes the specific tests planned, schedule, test location, planned/ needed facilities, and certification procedures.

d. Require development of contingency plans including replacements for legacy systems that may arrive late or with incomplete or inadequate "fixes."

e. Assume responsibility for emergency response capabilities to deal with Y2K problems beyond the competence of system owners and operators as they arise.

f. Require end-to-end analysis and testing of major scenarios to help define Y2K "system-of-systems" tests.

g. Require generation of test plans which include interfaces and relevant "homeless" systems.

h. Assure introduction of Y2K testing in every scheduled major test and exercise wherever possible.

4. Information Warfare [IW] Vulnerabilities

a. Alert all groups working on the Y2K problem to the potential for increasing system vulnerabilities to IW.

b. Bring the IW community into the Y2K arena. This should include active involvement of the IW Emergency Response Teams [ERTs].

c. Work with the IW community to see if there are ways of reducing current vulnerabilities with proper Y2K fixes.

5. Other Responsibiiities

a. Assume responsibility for distribution of reliable information on COTS hardware and software including tools.

b. Assume responsibility for promulgation of "fixes" and Y2K tools, including tool limitations and problems.

c. Be the focal point for dealing with commercial hardware/ SW firms on the

Y2K issue. Arrange for OSD [preferably the DepSecDef] to call in the CEOs of the relevant HW/SW companies and ask for their cooperation and help with this issue.

d. Assure that Y2K infrastructure considerations include consideration of the reliability of basic services at foreign bases.

e. Raise the awareness across DOD — consider implementation of a stand-down Y2K awareness/ testing day.

f. Assure appropriate interactions and coupling with other government agencies, such as FEMA, FAA, FCC, NIMA, State and Treasury.

g. Work with other government Departments to initiate some sort of Y2K education and awareness program for all countries with nuclear weapons, including, especially, China and Russia.

B. OSD should establish a Y2K "escape valve" fund under the direct control of the Y2K executive

1. The "escape fund" is to be made available for the following:

a. Critical "System of Systems" testing not planned for as part of "normal" testing.

b. Fixing critical "homeless" systems.

c. Replacement of legacy systems where this is critical and other program funds are not available.

d. Funding of special CINC needs

The fund should be established now and also included in the FY99 budget. It is not possible to estimate the funds required until the really critical systems have been identified, a meaningful reporting system has been established, and the relevant testing programs described. The total is, however, thought to be greater than $100 M.

2. Sources for this fund:

a. Because testing of Y2K systems must be given special priority, a portion of funds earmarked for OT and E for all systems [not just those having Y2K problems] should be used as a source for Y2K testing.
This testing is far more important than much of the routine OT&E testing carried out on programs.

b. If necessary, OSD should impose a tax across some or all of the DoD budget to augment the above resources.

Note: The DoD IG and Service audit agencies have a planned '98 effort of 85 man years to examine the status of the Department's Y2K work. Most of this effort should be attached to the senior management responsible for correction of the Y2K problems.

C. OSD should work with the components to establish incentives for Program Managers and the other key people

Incentives would provide the necessary attention and emphasis to the Y2K issue. Suggested actions are:

a. Extend tours for Program Managers and other key people to cover the period into year 2000 to assure continuity of management, technical, and resource attention through the testing and "solution" phases.

b. Provide extra payment in the form of bonuses for special situations where the accomplishments are of unusually great quality or where the required efforts cause undue hardships.

c. In anticipation of unusual time demands on key personnel during the next two plus years, modify the "use or lose" leave policy to allow ready exceptions for those personnel.

d. In cases where the Program Manager and/or other key personnel are reassigned before the Y2K critical dates occur, defer the comments on that portion of the fitness report until the degree of Y2K compliance has become evident.

The Task Force believes the Department needs to take these steps to get on top of the Y2K problem and to reduce substantially the associated risks.

Appendices

Appendix A: Terms of Reference

Appendix B: Members and Advisors

Appendix C: Dates and Agenda

Appendix D: Sub-panels – Leaders and Members

Appendix E: Briefings, Additional Material

Appendix F: Glossary

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-3010

ACQUISITION AND
TECHNOLOGY

JUL 9 1997

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference for the Defense Science Board Task Force on Year 2000

You are requested to form a Defense Science Board (DSB) Task Force on the Year 2000 (Y2K) to determine if the priorities assigned, resources allocated and funding strategy used to implement the Department's Y2K five phase process are sufficient to ensure all mission critical systems will function properly on, before and after January 1, 2000. You should specifically address the feasibility of Component strategies that propose the work can be done within current budgets through various options (e.g., by changing software maintenance priorities, by delaying software research and development efforts, etc.).

The Y2K Task Force will provide advice, recommendations, and supporting rationale that addresses the items below for OSD, the Military Departments, the Joint Staff, Unified and Specified Combatant Commands, Defense Agencies, and DoD Field Activities.

- Degree and quality of top-level and middle-level ownership and sponsorship for addressing the Y2K problem;

- Adequacy of resources:

  ⇒ Assigned to central project teams;

  ⇒ Allocated to implement the five phases (Awareness, Assessment, Renovation, Validation, and Implementation); and

  ⇒ Allocated to building and maintaining a DoD Y2K systems inventory.

- Adequacy of risk management strategies and controls to include sufficient early warnings to enable timely detection and correction;

- Adequacy of contingency planning;

- Adequacy of configuration management control procedures;
- Adequacy of renovation, testing/validation and deployment procedures;
- Adequacy of scheduling procedures and testing/validation facilities;
- Adequacy of information distribution about the Y2K status of application software packages, systems software and utilities;
- Adequacy of information distribution about automated Y2K tools; and
- Adequacy of quarterly reporting requirements to determine progress.

The Task Force should: (a) submit its final report by December 30, 1997; (b) include an assessment of the risks to mission critical systems; and (c) provide specific advice for implementation of the Task Force's recommendations.

The Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and I will co-sponsor this Task Force. Mr. Bert Fowler will serve as the Task Force Chairman. Mr. Walter Benesch will serve as the Executive Secretary and CDR David Norris, USN, will serve as the Defense Science Board Secretariat representative.

The Task Force will be operated in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5104.5, "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, United States Code, nor will it cause any member to be placed in the position of acting as a procurement official.

Joseph Eash
Acting Under Secretary of Defense
(Acquisition and Technology)

Appendix B: Members and Advisors

Members

Charles A. Fowler
C. A. Fowler Associates
Task Force Chair

David R. Heebner
Private Consultant
Task Force Vice-Chair

Walter P. Benesch
ASD(C^3I)/ Information Technology Directorate
Task Force Executive Secretary

Herbert W. Anderson
Northrop Grumman
Corporate Vice President of Data Systems and Services Division

Thomas K. Backman
MITRE Corp.,
Associate Director of Information Technologies Directorate

Dr. David L. Briggs
MIT/ Lincoln Laboratory,
Asst. Director for Air and Ballistic Missile Defense

Dr. George H. Heilmeier
Private Consultant

Dr. William G. Howard Jr.
Private Consultant

Brian T. Keane
Keane Inc.
Senior Vice President, Mid-Atlantic & Southern U.S. Branch Operations

W. Lily O'Byrne
Lockheed Martin,
VP of Applications, Enterprise Information Systems

Dr. Alan B. Salisbury
Learning Tree International President

John M. Stewart
McKinsey and Co.
Director

VADM Jerry O. Tuttle, USN (Ret.)
MANTECH Systems International Corp.
President

Dr. John H. Warner Jr.
SAIC
Executive Vice President and Director

Jack H. Winters
IBM
Vice President, IBM Global Services

Dr. Lawrence T. Wright
Booz-Allen and Hamilton,
Partner and Vice President

Advisors

Allan A. Astley
Defense Technical Information Center

Lt Col Ramona Barnes, USAF
Joint Staff, J-6

Margaret B. Bennardo
DoD Inspector General

Col Ray Brylski, USAF
AFCICI

CDR Gary Evans, USN
Deputy Assistant Secretary of Navy (C^4I)

Robin Frost
USD(A&T)/Dir, Test Systems Eng.

CAPT Karl Hartenstine, USMC
MCCTA

Steve Selwyn
ASD(C^3I)/ ISS

Dr. James Soos
ASD(C^3I)

Support

George M. McVeigh Jr.
SAIC

CDR Dave Norris, USN
Defense Science Board

Appendix C: Dates and Agenda

The Task Force met on the following dates:

September 15-16, 1997
October 16-17, 1997
November 6-7, 1997
December 1-2, 1997
January 12-13, 1998

Following are the agendas for those meetings:

Meeting — September 15, 16, 1997

September 15, 1997

8:30	Coffee/ Tea	
9:00	Chairman's opening remarks and introductions	
9:20	DSB Vice Chairman's Remarks	*Dr. Jacques Gansler*
9:40	Standards of Conduct Briefing	*General Counsel*
10:00	C^3I Overview: Y2K Problem ASD(C^3I)	*Dr. Jim Soos*
11:00	Break	
11:30	MITRE View	*Mr. Tom Backman*
12:00	Keane Inc, View	*Mr. Brian Keane*
12:30	Lunch	
1:00	SAIC	*Dr. John H. Warner, Jr.*
1:30	"Managerial and Political Implications of the Year 200 Fix,"	*Paul A. Strassmann, Strassmann, Inc.*
2:00	DSB Chairman's Remarks	
2:15	"Bellcore Year 2000 Integration Solution"	*Mr. Paul Minkin*
3:15	IBM	*Mr. Roger Andrews*
4:15	Discussion	
5:00	Adjourn	

September 16, 1997

8:00	Coffee/ Tea	
8:30	Discussion	
9:30	Service CIO Navy	*CDR Gary Evans*
10:30	Break	
11:00	Service CIO — Marines	*Maj Ken Beutel, Deputy Director, MCCTA*
12:00	Lunch	
12:30	Service CIO — Army	*Mr. Bill Dates, Army Y2K Program Manager*
1:30	Service CIO — Air Force	*Col Ray Brylski, Air Force Y2K POC*
2:30	Joint Staff CIO — J6	*Lt Col Ramona Barnes, J-6V, JCS*
3:30	Break	

3:00	Discussion
4:00	Planning Session
5:00	Adjourn

Meeting — October 16, 17, 1997

October 16, 1997

8:30	Coffee/ Tea	
9:00	Chairman's remarks	
9:15	Overview of last meeting	*Mr. George McVeigh, SAIC*
9:45	ASD(C^3I) Update	*Mr. Sam Worthington, Director Information Technology*
10:15	Break	
10:45	Aegis	*Mr. Bill Hyre with Mr. Jim Reagan*
11:45	ASD (C^3I)	*Mr. Tony Valletta, Acting ASD(C^3I)*
12:15	Lunch	
12:45	Patriot	*Mr. Dean Mullis*
1:45	F-15 E	*Col Richard Bowman, F-15 Program Office (ASC/FBA), Wright Patterson AFB OH and AFPEO/FB (Fighters and Bombers) with Maj Richard Ruggiero*
2:45	Break	
3:15	"GCCS Year 2000 Task Force"	*Maj. Eleazer, DISA*
4:15	Task Force Discussion	
5:00	Adjourn	

October 17, 1997

8:00	Coffee/ Tea	
8:30	Task Force Discussions	
9:30	Intelligence Community Outlook	*Ms. Letitia A. Long, Associated Executive Director, Intelligence Community Affairs*
10:30	Break	
11:00	DLA/Logistics	*Ms. Sandra King, DLA Y2K P.M., with Ms. Sarah Reed*
12:00	Lunch	
12:00	DFAS/Finance	*Mr. Bob Burke, Deputy Director for Information Management*
1:30	Task Force Discussion	
2:15	Break	
2:45	Task Force Discussion	
	Planning Future agenda	
4:00	Adjourn	

Meeting — November 6-7, 1997

November 6, 1997

8:30	Coffee/ Tea	
9:00	C^3I Update	*Mr. Tony Valletta, Acting ASD(C^3I)*
9:30	Group I — Process, monitoring, Resources	*Mr. Tom Backman*
10:00	Group II — Incentives, Replacement, Fixes	*Mr. Jack Winters*
10:30	Break	
10:45	CINCSTRATCOM,	*Col Rounce and Maj Healy, USAF, USSTRATCOM*
12:00	Group III — Testing, Contingencies, Emergency Response, Discussion	*Mr. Brian Keane*
12:30	Lunch	
1:00	Y2K Issues with GAO	*Mr. Jack Brock, Mr. John Stephenson, Mr. A Summers*
2:00	AWACS and JTIDS Brief	*Jim Lender, AWACS Program Office (MITRE), Linda Scannell, AWACS Program Office (MITRE), Maj David A. Huss, AFPEO/WS (Warning and Surveillance) Carmen A. Paludi, Jr., ESC/DIG, Maj. James Forney, ESC/DIG*
3:00	Informal Discussion of IG Status Report	*Mary Lu Ugone, DOD IG*
3:15	Break	
3:30	"Multiple Launch Rocket System (MLRS) Year 2000 Weapon Interface"	*Mr. Neal Patterson ,MLRS Project Office.*
4:30	Group V — Impact Y2K: Financial Operations, Logistics, Transportation	*Mr. Herb Anderson*
5:30	Adjourn	

November 7, 1997

8:00	Coffee/ Tea	
8:30	Discussion	*Members and Advisors*
9:00	Group IV — Information Warfare Vulnerabilities	*Dr. Larry Wright*
9:30	Group VI — Impact Y2K: C^3, Weapons Systems, CINCs	*Mr. John Warner*
10:00	BREAK	
10:15	Group VII — Impact Y2K: Intelligence Systems	*Dr. Larry Wright*
11:00	MIT Presentation	*Dr. Howard Shrobe*
12:00	Lunch	
12:30	JTICs Role in Y2K	*Dr. Carl Palmer*
1:30	DOD/ USG Telecom Infrastructure	
2:15	Break	
2:45	Task Force Discussion	*Members and Advisors*
4:00	Adjourn	

Meeting — December 1, 2, 1997

December 1, 1997

8:30	Coffee/ Tea	
9:00	Chairman's time	*Mr Bert Fowler*
9:30	Task Force Discussions	
10:00	"Tools for Resolving Year 2000"	*Howard Shrobe, MIT*
11:00	"Software Test Verification: Key to Y2000 Readiness Assurance"	*Paul Strassmann, Software testing Assurance Corporation*
12:15	Lunch	
12:45	Task Force Discussions	
2:45	Break	
3:15	Task Force Discussions	
5:00	Adjourn	

December 2, 1997

8:00	Coffee/ Tea	
8:30	Chairman's time	
9:00	Task Force Discussions	
10:15	C^3I Update	*Tony Valletta, Actg. ASD(C^3I)*
11:00	J-6V	
11:45	Lunch	
12:15	Navy E-6	
1:00	Task Force Discussions	
3:00	Break	
3:15	Task Force Discussions	
4:00	Adjourn	

Meeting – January 12-13, 1998

January 12, 1998

8:30	Coffee/ Tea	
9:00	ASD(C^3I) Update	Tony Valletta, Actg. ASD(C^3I)
10:00	Task Force Discussions	
10:15	Break	
10:30	Task Force Discussions	
11:15	National Security Agency	*Ms. Bambi Nelms*
12:15	Lunch	
12:45	JITC: Subject Testing	*Mr. Leo Hansen*
2:45	Break	
3:15	Task Force Discussions	
5:00	Adjourn	

January 13, 1998

8:00	Coffee/ Tea
8:30	Chairman's time
9:00	Task Force Discussions
10:15	Break
10:45	Task Force Discussions
12:00	Adjourn

Appendix D: Sub-Panels — Leaders and Members

Sub-Panels

Process Monitoring, Resources
W. Lily O'Byrne*
Thomas K. Backman

Incentives, Replacement, Fixes
Jack H. Winters*
John M. Stewart

Testing, Contingencies, Emergency Response
Dr. William G. Howard Jr.*
Brian T. Keane
Dr. David L. Briggs

Information Warfare Vulnerabilities
Dr. Lawrence T. Wright*
Charles A. Fowler

Impact Y2K: Financial, Logistics, Transportation
Herbert W. Anderson*
Dr. Allen B. Salisbury

Impact: C^3, Weapon Systems, CINCs
Dr. John H. Warner Jr.*
VADM Jerry O. Tuttle, USN (Ret)
David R. Heebner

Impact Y2K: Intelligence Systems
Lawrence T. Wright*
Charles A. Fowler

Senior Advisor
Dr. George Heilmeier

* Sub-Panel Leader

Appendix E. List of Acronyms

A

AFCIC	Air Force Communications and Information Center
AFPEO	Air Force Program Executive Office
AFPEO/FB	Air Force Program Executive Office (Fighters and Bombers)
AFPEO/WS	Air Force Program Executive Office (Warning and Surveillance)
ASC	Aeronautical Systems Center
ASD	Assistant Secretary of Defense
AUTODIN	Automatic Digital Network
AWACS	Airborne Warnings and Control System

C

C^3	Command, Control, Communication
C^3I	Command, Control, Communication, and Intelligence
C^4I	Command, Control, Communication, Computers and Intelligence
CEO	Chief Executive Officer
CINCs	Commander-in-Chiefs
CIO	Chief Information Officer
CMS	Community Management Staff
COTS	Commercial Off The Shelf

D

DCI	Director of Central Intelligence
DCTF	Defense Communications Test Facility
DDI	Deputy Director Information
DFAS	Defense Financial and Accounting Agency
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISA/GCCS	Defense Information Systems Agency, Global Command and Control System
DISN	Defense Information Systems Network
DIST	Defense Information Support Tools
DLA	Defense Logistics Agency
DMIM	Defense Medical Information Management
DMS	Defense Messaging System
DOD	Department of Defense
DRI	Defense Reform Initiative
DSB	Defense Science Board

E

EKMS	Electronic Key Management System
ERTs	Emergency Response Teams

G

GAO	General Accounting Office
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GOTS	Government Off The Shelf

H

HQMC	Head Quarters Marine Corp.

I

IBM	International Business Machines
IPT	Integrated Product Team
IT	Information Technology
IW	Information Warfare
IV&V	Independent Validation and Verification

J

JCS	Joint Chiefs of Staff
JCS(J6)	Joint Chiefs of Staff/ J-6 (Command, Control, Communications, and Computers)
JITF	Joint Integration Test Facility
JTIC	Joint Interoperability Test Center
JTIDS	Joint Tactical Information Distribution System
JWID	Joint Warrior Interoperability Demonstrations

M

MHS	Military Health System
MIT/LL	Massachusetts Institute of Technology/ Lincoln Laboratory
MLRS	Multiple Launch Rocket System
MTF	Message Text Format

N

NATO	North Atlantic Treaty Organization
NIMA	National Imagery and Mapping Agency
NRO	National Reconnaissance Office
NSA	National Security Agency

O

O&M	Operations and Maintenance
OASD (HA)	Office of the Assistant Secretary of Defense Health Affairs
OPNAV	Operations Staff Navy
OPR	Office of Primary Responsibility
OSD	Secretary of Defense
OT&E	Operational Test and Evaluation

P

PACOM	Pacific Command
PCs	Personal Computers

R

R&D	Research and Development

S

SAIC	Science Applications International Corporation
SAs	System Administrators
SECDEF	Secretary of Defense

STU-III	-	Secure Telephone Unit-III

T

TOR		Terms of Reference

U

U.S.		United States
USACOM		United States Atlantic Command
USAF		United States Air Force
USD(A&T)		Under Secretary of Defense Acquisition and Technology
USN		United States Navy
USSOCOM		United States Special Operations Command
USSTRATCOM		United States Strategic Command

W

WARM		War Reserve Mode
WPAFB-OH		Wright Patterson Air Force Base, Ohio

Y

Y2K		Year 2000

NATION[redacted]FRASTRUCTURE PROTECTION CENTER (NIPC)
TRA[redacted]G, OUTREACH AND STRATEGY SECTION

DATE: 10/11/99

b6
b7C

____	7142	____	COMPUTER INVESTIGATIONS UNIT
____	7116		
____	7116		
____	7110	____	SPECIAL TECHNOLOGIES UNIT
____	7110		UC [redacted]
____	11741		
____	4012	____	CYBER EMERGENCY SUPPORT TEAM
____	7443		UC [redacted]
____	11719		
		____	ANALYSIS AND INFORMATION SHARING UNIT
____	11741		UC [redacted]
____	4825		
____	11719	____	WATCH AND WARNING UNIT
____	11719		UC [redacted]
____	7648		
____	5222	____	STRATEGY AND PLANNING UNIT
____	5849		UC [redacted]
____	4042	____	OUTREACH AND FIELD SUPPORT UNIT
____	11719		UC [redacted]
____	7373		
____	11526	____	TRAINING AND CONTINUING EDUCATION UNIT
			UC [redacted]
____	4042		
____	7139		
		____	[redacted]
____	11719		
____	11719	____	
____	11719		
		____	
____	11719		
____	11526		
____	11719	____	
____	11719		
____	11526	____	
____	11526		

COMMENTS

Please file. Thank you.

____ PLEASE CALL ME
____ PLEASE DISCUSS WITH ME
__✓__ APPROPRIATE ACTION
____ FOR YOUR INFORMATION
____ FOR YOUR APPROVAL
____ PLEASE PREPARE RESPONSE

RONALD L. DICK, SECTION CHIEF
TRAINING, OUTREACH AND STRATEGY SECTION
ROOM 11526, EXT. 6301

NATIONAL INFRASTRUCTURE PROTECTION CENTER (NIPC)
TRAINING, OUTREACH AND STRATEGY SECTION

DATE: SEPTEMBER 13, 1999

b6
b7C

[redacted]

[redacted]

COMMENTS

ATTACHED FOR YOUR APPROVAL IS AN EC ENTITLED "Y2K CRISIS CONTINGENCY PLANNING." UPON APPROVAL, PLEASE CALL [redacted] EXT. 6301, WHO WILL WALK THE EC TO THE NEXT APPROVING OFFICIAL. THANK YOU.

b6
b7C

_____ PLEASE CALL ME
_____ PLEASE DISCUSS WITH ME
XXXXXXXX APPROPRIATE ACTION
_____ FOR YOUR INFORMATION
XXXXXXXX FOR YOUR APPROVAL
_____ PLEASE PREPARE RESPONSE

RONALD L. DICK, SECTION CHIEF
TRAINING, OUTREACH AND STRATEGY SECTION
ROOM 11526, EXT. 6301

PLS. INITIAL THE ROUTING SLIP AND EC.

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 09/23/1999

To: Director's Office	**Attn:** [redacted]	b6 b7C
All Field Offices	ADIC (Personal Attn); SAC (Personal Attn); NIPCI Coordinators/Managers; Key Asset Coordinators; Crisis Mgmt Coordinators; WMD Coordinators CART Coordinators	
All Legats	Legal Attache	
Administrative Services	AD Ruben Garcia, Jr.	b6 b7C
Criminal Investigative	SC Richard D. Robillard	
CJIS	AD David R. Loesch	
Finance	Acting AD [redacted]	
Information Resources	AD Carolyn G. Morris	
Inspection	AD Wiley D. Thompson, III	
Laboratory	AD Donald M. Kerr, Ph.D.	
National Security	SC Charles H. Middleton SC Timothy Bereznay SC James D. Ohlson	
EEO	[redacted] EEO Officer	
General Counsel	GC [redacted]	
OPCA	AD John E. Collingwood	
Training	AD Jeffrey Higginbotham	

From: National Security
CEST/CIOS/NIPC, Room 11719
Contact: [redacted] (202) 324-0331

Uploaded 9/23/99 [redacted]

To: All Field Offices From: National Security
Re: [redacted] 09/23/1999

b6
b7C
b3
b7E

Approved By: [redacted]

Dick Ronald L

[redacted]

Drafted By: Vanzant David A:dav

Case ID #: [redacted] (Pending)
294I-HQ-1270744-102

Title: Y2K Crisis Contingency Planning

Synopsis: To provide guidance for Y2K Crisis Contingency planning and preparation for the year-end date change. This document highlights the following activities for all Field Offices to undertake in connection with captioned matter:

- The development and implementation of a plan and command center for the Y2K rollover.

- The coordination and liaison with Y2K points of contact in each of the Federal Emergency Management Agency (FEMA) ten Regional Offices and each office of the State Emergency Management Director.

b3
b7E

• Reporting of information regarding possible malicious activity around the millennium rollover, including potential cyber attacks on the nation's infrastructures as well as to review referral of potential physical attacks from millennial or other groups, and the status of FBI systems, to FBIHQ for analysis and timely conveyance to the Information Coordination Center (ICC) and other field divisions/Legats, as appropriate.

Reference: [redacted]

Enclosure(s): Enclosed for all receiving offices and Legats are the following:

1. A copy of the Y2K Cyber Intrusion Incident Reporting (CIIR) Form.

2. A copy of the list of the National Emergency Management Association 1999-2000 Membership Roster.

3. A copy of FEMA's Regional Offices.

4. A copy of FEMA's guide for State and Local Emergency Managers titled "***Contingency and Consequence Management Planning for Year 2000.***"

Details: Presidential Decision Directive (PDD) 63, Critical Infrastructure Protection, states "The National Infrastructure Protection Center (NIPC) will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts." The National Infrastructure Protection and Computer Intrusion Program (NIPCIP) implements this national responsibility. It assigns investigative and response activities to the National Infrastructure Protection Computer Intrusion (NIPCI) squads/teams in FBI Field Offices.

In order to fulfill this national responsibility during the date change, when there is a chance of increased malicious cyber activity, the NIPC is developing and coordinating Y2K cyber-crisis contingency planning within the FBI, in coordination with other Government Agencies.

To: All Field Offices From: National Security
Re: [redacted] 09/23/1999

b3
b7E

The NIPC will operate a Y2K Command Post (CP), on a 24-hour basis, starting 12/29/1999, and continuing through 1/5/2000. Located in the Strategic Information and Operations Center (SIOC) at FBIHQ, Y2K CP contact can be made through the NIPC Watch and Warning Unit: telephone (202) 323-3204; secure telephone (202) 323-2204; fax (202) 323-2079; and secure fax (202) 323-2080; or e-mail nipc.watch@fbi.gov.

The Y2K CP at FBIHQ will also include representation from the Computer Analysis and Response Team (CART), Violent Crimes and Major Offenders (VCMO) Section, Domestic Terrorism (DT) Section, International Terrorism (IT) Section, the Financial Crimes (FC) Section and the appropriate Counterintelligence Sections, in an effort to provide assistance and guidance to the field for non-cyber related events which may occur as a result of, or under the guise of, the millennium rollover. Representatives from these sections will function in a liaison capacity to ensure complete and effective program management by the respective program managers of events, such as physical attacks on the infrastructure or significant fraudulent activities occurring on the Internet, during the operation of the Y2K CP. In addition, [redacted] Inspection Division, who has coordinated the FBI's Y2K preparedness concerning the bureau's own information systems, will also be represented in the Y2K CP to handle the reporting, and appropriate response, for any Y2K outages in FBI systems.

b6
b7C

The FBIHQ Y2K CP is being established to provide FBI executive management with the ability to collect information regarding possible malicious activity around the millennium rollover. This will include potential cyber attacks on the nation's infrastructures as well as to review referrals of potential physical attacks from millennial or terrorist groups.

The NIPC is also working with the National Security Agency, Department of Defense and private entities in an attempt to develop a guide to methods and procedures, for use by the Field Offices, in assessing potential Y2K cyber incidents. Currently, this guide does not exist. It is anticipated the guide will include methods by which an initial assessment can be made to determine whether an incident is maliciously induced, as opposed to a Y2K software problem, which is not under the responsibility of the FBI. When produced, it will be provided to the field via separate communication.

b3
b7E

The responsibility of the FBI is to investigate incidents or intrusions that are criminal in nature or have National Security implications. The FBI is **not responsible** for incidents that are caused purely by Y2K outages - i.e. computer systems' failure to handle the date rollover. However, the Field Office should track all complaints received from 12/29/1999, through 1/5/2000, regarding Y2K incidents. The Field should categorize these complaints into three areas:

1. Y2K malicious events where further investigation is required and a case is opened.

2. Undetermined, meaning that no determination can be made as to whether the incident is purely a Y2K outage or is malicious in intent and an investigation is initiated to obtain sufficient information to determine if the incident is malicious or a purely Y2K outage.

3. Purely Y2K related and no investigative response is required, however the complaint should be referred to the respective State Emergency Management Office or FEMA Regional Office.

In each instance an FD-801 is to be completed and immediately faxed to the NIPC Watch, fax (202) 323-2079, or secure fax (202) 323-2080, or the information may be telephonically relayed to the NIPC Watch through telephone number (202) 323-3204 with the FD-801 to follow.

If the Field Office receives information concerning a Y2K outage, rather than a malicious incident, they should refer the complainant to their respective State Emergency Operations Center (EOC) or their FEMA Regional Office. In addition, the Field Office should submit an FD-801, to the NIPC Watch, documenting the nature of the complaint and the appropriate resolution/referral of that complaint.

Field Office Y2K Planning

Each Field Office is requested to establish and staff a CP to address anticipated malicious activity around the date change, in accordance with established crisis plans. Each Field Office should ensure that their command post is structured to

b3
b7E

handle both cyber and physical events which may occur during the millennium rollover, as the FBIHQ Y2K Command Post is structured. The Field Office CP should be manned 24 hours a day starting no later than 12/31/1999, and continuing through at least 01/03/2000. Decisions concerning the level of staffing are being left to the discretion of individual SAC's, based on local conditions and requirements for their respective CP. However, each Field Office is to ensure that appropriate investigative and analytical personnel, knowledgeable of cyber related matters, staff their respective Field Office CP.

Each Field Office should ensure that at least one CART Examiner is on stand-by during the millennium rollover.

Each Field Office is requested to advise the NIPC of the procedure to be used for handling complaints and how coordination with the Y2K CP and other local and Federal emergency agencies, including the Federal Emergency Management Agency (FEMA), is going to be handled. A guide for State and Local Emergency Managers titled "***Contingency and Consequence Management Planning for Year 2000***" was published by FEMA in February 1999, and maybe useful. A copy of this document is enclosed with this communication. It is also available at www.fema.gov.

As stated in referenced EC, each Field Office should have submitted a written Y2K Contingency Plan. If this has not been completed, Field Office management should ensure submission as quickly as possible.

It is anticipated that events and reporting will be handled through normal investigative channels. However, each Field Office should consider what alternate means of communication to the Y2K CP are available. In anticipation of the possibility of disruption to normal communication capability, the NIPC will be providing, under separate cover, satellite telephones for use to communicate with the FBIHQ Y2K CP in the event that telecommunications capabilities are impaired.

The enclosed Cyber Intrusion Incident Reporting (CIIR) Form should be provided to Non-FBI entities, such as Key Assets, public contacts, and other law enforcement agencies, to facilitate the reporting information to the Field Office concerning cyber intrusion incidents. Each Field Office is

b3
b7E

requested to provide this CIIR Form to the appropriate entities. They should be advised to provide this information, or have this type of information ready, if they report an intrusion or cyber incident to the Field Office.

In lieu of developing a new form for reporting Y2K related matters to FBIHQ, Field Offices will use the FD-801 report to report Y2K related complaints and computer intrusion incidents. From 01/01/2000, until at least 08/31/2001, the remarks section of the FD-801 should include responses to the following questions regarding Y2K for all intrusion incidents:

1. Have you had your system prepared/replaced/updated for Y2K?

2. If yes? Who conducted the work (Point of Contact information)? When was the work conducted?

3. Have you had this problem before?

4. What is status of your system?

5. What Types of Software do you utilize (Off the shelf, Proprietary)? If Proprietary, System Managers POC information.

6. Who maintains your systems (POC information)?

WMD Coordinators - Response to Physical Act of Terrorism

During the Fall of 1998, two ECs from the Domestic Terrorism/Counterterrorism Planning Section directed all WMD Coordinators to contact state and local authorities and conduct joint planning for responding to acts of terrorism, specifically WMD events. Planning included the development and implementation of WMD Incident Contingency Plans (WMDICP) for every Division, and a Nuclear Site Security Plan (NSSP) for those offices with DOE/Nuclear facilities within their respective territories. These plans were to be added as an annex to each Division's Crisis Response Plan. Field offices should assess their progress on these matters and review current plans. WMD Coordinators are responsible for ensuring that their respective WMDICP is current and that liaison has been established with the appropriate officials from the various federal, state and local agencies who

b3
b7E

would be involved in either the crisis and/or consequence management aspects of a mass casualty/WMD event. In addition, WMD Coordinators are encouraged to meet with the field office's crisis management team, to include the NIPC Coordinator, Key Asset Coordinator and the Crisis Management Coordinator, to ensure that each member is familiar with their respective WMDICP and NSSP, as appropriate, and to review the response structure for their field office.

State Emergency Management Offices

Each State, in coordination with its FEMA Regional Office is developing a contingency plan in preparation for the potential impact of the Y2K millennium rollover. Each field office is requested to coordinate with the State Emergency Management Director or the Director's Y2K point of contact and:

1. Inform the State of our responsibility in responding to malicious activity that is criminal in nature or has national security implications.

2. Offer FBI liaison support in the State Emergency Operations Center (EOC), during its operation.

A list of the State Emergency Management Directors and telephoned numbers is enclosed with this communication. For the States that have more than one Division the following offices will have responsibility for their State EOC liaison:

1. Sacramento Division for California
2. San Antonio Division for Texas
3. Jacksonville Division for Florida
4. Memphis Division for Tennessee
5. Springfield Division for Illinois
6. Cincinnati Division for Ohio
7. Richmond Division for Virginia
8. Albany Division for New York
9. Kansas City Division for Missouri
10. Phoenix Division for Arizona
11. Philadelphia Division for Pennsylvania

Each of these Divisions should coordinate with the other Divisions located in their respective States and advise the NIPC of how communications will be handled between affected

b3
b7E

offices. FBI Liaisons to the State EOC's should report relevant information back to their respective Field Office which should then pass the information to the Y2K CP at FBIHQ. Enclosed with this communication is a list, by State, of EOC's.

Information Coordination Center (ICC)

The Y2K CP at FBIHQ will be the sole liaison for all direct FBI communications with ICC. No Field Offices will provide any information regarding status of FBI Systems, FBI facilities or FBI investigations to the ICC or FEMA. Field Offices should report immediately all internal systems status information to the Y2K CP.

The Information Coordination Center (ICC) of the President's Council on Year 2000 Conversion will be the Federal Government's central point for gathering information concerning year 2000 conversion, and analyzing and summarizing information on system operations during the Y2K date rollover for purely Y2K related events and statuses. Malicious activities or unknown causes of Y2K events will be referred to the NIPC. The ICC has been established to provide the Federal Government with an ability to collect and coordinate, in one location, information about system operations during the Y2K transition, from across the government and the economy. It should be noted that the ICC is not responsible for investigating malicious activity.

The ICC will work with government and industry information and emergency operations centers to gather and disseminate information on system operations during the date rollover. This dissemination will include private and public entities such as the **news media.**

Industry information centers will provide data to the ICC through the appropriate Federal agencies. For example, the electric power industry will report to the Department of Energy on the status of power companies. DOE will, in turn, provide that information to the ICC. Individual Federal agencies, such as DOE, will also provide the ICC information about the status of their own systems and programs. Internationally, information from the Departments of State and Defense, as well as national Y2K coordinators from around the world, will add to the data being gathered through industry information centers.

b3
b7E

The ICC will track the date rollover status of vital Federal Government systems (e.g., Social Security check processing systems, DOD early warning systems, FAA air traffic control systems), State and local government systems, and critical public and private sector systems that support key infrastructures. The ICC will also gather information about how important international systems handle the transition to the year 2000.

The ICC will divide basic information concerning systems into two categories: systems that are operating normally and systems that are not. For a system that is not operating normally, the ICC will gather information on the nature of Y2K-related problems affecting the system, the severity of those problems, and efforts underway to resolve them.

The FBIHQ Y2K CP will not provide the ICC with information relative to the status of State and local emergency and law enforcement systems, inasmuch as this information will be reported to the State EOC and these State EOCs will report it to the ICC. Malicious attacks on State and local government systems, however, are to be reported to the NIPC by the respective Field Office and an appropriate investigative response is to be initiated by that Field Office. This matter has been discussed with the Emergency Law Enforcement Sector Forum, a group established by PDD 63 and chaired by the NIPC.

FEMA Regional Offices

Field Offices should endeavor to make clear to their contacts the distinction between the roles of the ICC and the FBI, because of potential confusion that might be caused by inaccurate statements from other entities. It should be made clear that the FBI is responsible for responding to malicious activity that is criminal in nature or has national security implications, while the ICC is responsible for handling information concerning Y2K outages caused by software problems. The NIPC will be in close communication with the ICC to exchange any relevant information, as appropriate.

FEMA has ten regional offices. Each regional office is working directly with the States in developing contingency and consequence management plans for the Year 2000 conversion. Each of the following Field Offices should coordinate with the

b3
b7E

appropriate FEMA Regional Director or the Director's Y2K point of contact and:

1. Inform the Director of our responsibility in responding to malicious activity that is criminal in nature or has national security implications.

2. Offer FBI Liaison support in the Regional Operations Center (ROC) during its operation.

The following is a list of the ten ROCs and the respective Field Office for coverage:

Region I (Boston) - Boston
Region II (New York) - New York
Region III (Philadelphia) - Philadelphia
Region IV (Atlanta) - Atlanta
Region V (Chicago) - Chicago
Region VI (Denton) - Dallas
Region VII (Kansas City) - Kansas City
Region VII (Denver) - Denver
Region IX (San Francisco) - San Francisco
Region X (Bothell) - Seattle

A list of the Regional Directors and their Y2K points of contact are enclosed with this communication.

Field Offices should provide Liaison support to the ROC during its hours of operation. The liaison will report any relevant information to the Y2K CP at FBIHQ and inform the other FBI Liaison representatives at the State EOC and/or other locations of the same information.

FEMA will be the principal Federal agency for gathering Y2K information from State and local governments and will in turn provide that information to the ICC. FEMA will employ and operate under the current procedures outlined in the Federal Response Plan (FRP). While the FRP is not designed to meet the technological support to the owner/operator of a disrupted system, it does include as designed support and emergency assistance to State and local governments. The focus remains the same, i.e. States can continue to perform essential community services, such as issuing emergency warnings, dissemination

b3
b7E

public health and safety information, carrying out health and safety measures, reducing immediate threats to public health and safety, providing temporary housing assistance, and distributing medicine, food, and other goods to meet basic human needs.

Public Outreach

Each Field Office is requested to conduct a Public Information campaign in coordination with FEMA Regional Offices and State Emergency Management Directors to inform the public in their respective jurisdiction about:

1. What responsibilities the FBI will/will not have.

2. As appropriate, what measures that the respective Field Office is taking during the Y2K event.

3. How to contact the FBI Field Office CP.

This campaign should, for appropriate parties, provide the enclosed Cyber Intrusion Incident Reporting (CIIR) Form, and information concerning what to report and what not to report to the FBI.

Each office should provide the public with the following statement when asked about the FBI's Y2K initiative:

"The FBI will be setting up a Y2K Command Post at FBI Headquarters that will be staffed 24 hours a day starting 12/29/1999, and continuing through 1/5/2000. Each Field Office will also have staff at the millennium rollover, available to handle any potential criminal or national security incidents that might occur during the rollover period. The role of the FBI for the millennium rollover is to investigate incidents or intrusions that are criminal in nature or have National Security implications. These types of incidents should be reported to your local FBI Field Office (contact information). Any incidents reported which are solely caused by software problems and are not purposeful or malicious in nature should be referred to the State Emergency Operations Center (EOC) or the FEMA Regional Office." (contact information)

 b3 b7E

If questions are asked on how to distinguish between purely Y2K events and malicious events the following could be used as a guideline:

"The FBI is working on methods to distinguish Y2K related events from malicious or criminal events. There is no single answer to this question, since each situation is different. Common sense plays a big role in determining the source of the problem. Answers to the following questions may help separate Y2K events from malicious activities:

1. How is the system functioning? Have you had this problem before? What Computer/Systems are affected? Was there any damage?

2. If the system is connected to a network, when disconnected, does the problem stop?

3. What is different from pre 01/01/2000 and current operations?

These are some of the types of questions that need to be asked before you report the incident to anyone."

Legats Y2K Planning

Each Legat should contact their host law enforcement and security entities regarding Y2K issues and be prepared to receive lead information regarding Y2K related incidents. The Year 2000 Program Office has instructed IRB to request the [redacted] to provide the embassy contingency plans for each embassy where a Legat is housed. These plans, when received, will be maintained and available to us in the SIOC. They will be maintained by SIOC. It is also requested that the NIPC be provided information concerning contingency plans, within the embassy, for the millennium rollover. b7E

It is requested that all Legats provide the Y2K CP a status of their respective country's infrastructure (telecommunications, electrical, water, etc..), and overall assessment of problems that may exist as soon as possible but no later that 9:00 a.m. (local country time) on 1/1/2000.

To: All Field Offices From: National Security
Re: [redacted], 09/23/1999 b3 b7E

Legats should provide the following information to inquiries regarding the FBI Y2K initiatives:

"The FBI will be setting up a Y2K Command Post at FBI Headquarters that will be staffed 24 hours a day starting 12/29/1999, and continuing through 1/5/2000. Each Field Office will also have staff at the millennium rollover available to handle potential criminal or national security incidents that might occur during the rollover period. The role of the FBI for the millennium rollover is to investigate incidents or intrusions that are criminal in nature or have National Security implications."

Numerous issues will be identified in the future for which further guidance will be provided. However, questions regarding this communication or the operation of the Y2K CP can be referred to Supervisory Special Agent (SSA) [redacted] b6 b7C Cyber Emergency Support Team (CEST), Computer Investigations and Operations Section (CIOS), telephone number (202) 324-0331, SSA [redacted] Chief, CEST, CIOS, telephone number (202) 324-9174, SSA [redacted] Chief, Outreach and Field Office Support Unit (OFSU), Training, Outreach and Strategy Section (TOSS), telephone number (202) 324-6303, Ronald Dick, Chief, TOSS, telephone number (202) 324-6302, or [redacted] Chief, CIOS, telephone number (202) 324-0301.

b3
b7E

LEAD(s):

Set Lead 1:

ALL RECEIVING OFFICES

a) Within the parameters set out above, all Field Offices are requested to establish and staff a CP to address the anticipated Y2K related events. Provide Field Office CP structure, staffing and contact information to the NIPC.

b) Advise the NIPC how complaints and coordination with the Y2K CP at FBIHQ and other local and Federal emergency agencies, including the Federal Emergency Management Agency (FEMA) are going to be handled.

c) Advise the NIPC of their respective call-out plan for personnel.

d) The Field Office CP should be prepared to provide the Y2K CP an update of complaints by category every four hours starting at 12:30 p.m. 12/29/99.

Set Lead 2:

ALL RECEIVING OFFICES

Conduct a Public Information campaign to inform their jurisdiction about what services Field Offices will/will not provide and what measures they are taking during the Y2K event. This campaign should provide a format for incident reporting to the FBI, what to report and what not to report to the FBI.

Set Lead 3:

ALL RECEIVING OFFICES

a) Utilizing the enclosed list of EOC's and guidelines set out above, Field Offices are requested to make appropriate contacts to arrange FBI representation and obtain staffing and contact information for the transmittal to NIPC by 10/18/1999.

b) Utilizing the enclosed list of FEMA Regional Directors and Y2K Points of Contact and guidelines set out above,

b3
b7E

Field Offices are requested to make appropriate contacts to arrange FBI representation and obtain staffing and contact information for the transmittal to NIPC by 10/18/1999.

Set Lead 4:

ALL Legats

Contact their host law enforcement entities regarding Y2K issues and be prepared to receive lead information regarding Y2K related incidents. It is also requested that the NIPC be provided information on Legat/Embassy contingency planning for the millennium rollover.

Provide the Y2K CP a status report of their respective country's infrastructure, and overall assessment of problems that may exist as soon as possible, but no later that 9:00 a.m. (local country time) on 1/1/2000.

♦♦

FEMA Regional Offices

Region	Director	Address	Y2K Point of Contact
I	Jeffery A. Bean	442 J.W. McCormack POCH Boston, MA 02109 (617) 223-9540	[redacted]
II	Lynn G. Canton	26 Federal Plaza New York, NY 10278 (212) 225-7209	[redacted] (212) 225-7018
III	Rita A. Calvan	Liberty Square Bldg 2nd Floor, 105 S. Seventh Street Philadelphia, PA 19106 (215) 931-5608	[redacted]
IV	John B. Copenhaver	3003 Chamblee Tucker Rd Atlanta, GA 30341 (770) 220-5200	[redacted] (912) 225-4572
V	Dale Shipley	536 S. Clark Street, 6th Floor Chicago, IL 60605 (312) 408-5501	[redacted] (312) 408-5582
VI	R.L. (Buddy) Young	FRC 800 North Loop 288 Denton, TX 76201 (940) 898-5104	[redacted]
VII	John A. Miller	2323 Grand Avenue, Suite 900 Kansas City, MO 64108 (816) 283-7582	[redacted] (816) 283-7010
VIII	Richard P. Weiland	Denver Federal Center Bldg 710, Box 25267 Denver, CO 80225 (303) 235-4967	[redacted] (303) 235-4864
IX	Martha Whetstone	Bldg 105, Presidio of San Francisco San Francisco, CA 94129 (415) 923-7100	PT&E Division [redacted]
X	David L. deCourcey	Federal Regional Center 130 228th Street, SW Bothell, WA 98201 (425) 487-4604	[redacted] (425) 487-4603

b6
b7C

NATIONAL EMERGENCY MANAGEMENT ASSOCIATION
1999 - 2000 MEMBERSHIP ROSTER

State Members

ALABAMA (Region IV)
M[redacted]
Acting Assistant Director
Emergency Management Agency
5898 County Road 41, P.O. Drawer 2160
Clanton, AL 35046-2160
(205) 280-2201 FAX (205) 280-2410
[redacted]@aema.state.al.us

ALASKA (Region X)
Mr. Dave Liebersbach
Director
Division of Emergency Services
P.O. Box 5750
Fort Richardson (Anchorage), AK 99505-5750
(907) 428-7058 FAX (907) 428-7081
[redacted]@ak-prepared.com

ARIZONA (Region IX)
Mr. Michael P. Austin
Director
Division of Emergency Management
5636 E. McDowell Road
Phoenix, AZ 85008
[redacted]
[redacted]@dem.state.az.us
www.state.az.us/es

ARKANSAS (Region VI)
Mr. W.R. "Bud" Harper
Director
Department of Emergency Management
P.O. Box 758
Conway, AR 72033
[redacted]
[redacted]@adem.state.ar.us

CALIFORNIA (Region IX)
Mr. Dallas Jones
Director
Governor's Office of Emergency Services
2800 Meadowview Road
Sacramento, CA 95832
(916) 262-1816 FAX (916) 262-2837
[redacted]@oes.ca.gov

COLORADO (Region VIII)
Mr. Tommy F. Grier b6
Director b7C
Office of Emergency Management
15075 S. Golden Road
Golden, CO 80401-3979
(303) 273-1622 FAX (303) 273-1795
[redacted]@state.co.us

CONNECTICUT (Region I)
Mr. Daniel McGuire
Director
Office of Emergency Management
Department of Public Safety
360 Broad Street
Hartford, CT 06105
(860) 566-3180 FAX (860) 247-0664
[redacted]@juno.com

DELAWARE (Region III)
Mr. Sean Mulhern
Director
Emergency Management Agency
165 Brick Store Landing Road
Smyrna, DE 19977
(302) 659-3362 FAX (302) 659-6855
[redacted]@state.de.us

DISTRICT OF COLUMBIA (Region III)
Mr. Peter LaPorte
Director
Emergency Management Agency
2000 14th Street, NW, 8th Floor
Washington, DC 20009
(202) 727-3159 FAX (202) 673-2290
[redacted]@dcg.org

FLORIDA (Region IV)
Mr. Joseph F. Myers
Director
Division of Emergency Management
2555 Shumard Oak Boulevard
Tallahassee, FL 32399-2100
(850) 413-9969 FAX (850) 488-1016
[redacted]@dca.state.fl.us

NATIONAL EMERGENCY MANAGEMENT ASSOCIATION
1999 - 2000 MEMBERSHIP ROSTER

GEORGIA (Region IV)
Mr. Gary McConnell
Director
Emergency Management Agency
P.O. Box 18055
935 East Confederate Avenue, S.E.
Atlanta, GA 30316-0055
(404) 635-7000 FAX (404) 635-7205
[redacted]@gema.state.ga.us
www.state.ga.us/GEMA/

HAWAII (Region IX)
Mr. Roy C. Price, Sr.
Vice Director
State Civil Defense
3949 Diamond Head Road
Honolulu, HI 96816-4495
(808) 733-4300 FAX (808) 733-4287
[redacted]@state.hi.us

IDAHO (Region X)
Mr. John Cline
Director
Bureau of Disaster Services/Military Division
4040 Guard Street, Bldg. 600
Boise, ID 83705-5004
(208) 334-3460 FAX (208) 334-2322
[redacted]@bds.state.id.us
www.state.id.us/bds

ILLINOIS (Region V)
Mr. Mike Chamness
Director
Emergency Management Agency
110 E. Adams Street
Springfield, IL 62701-1109
(217) 782-2700 FAX (217) 524-7967
[redacted]@pop.state.il.us
www.state.il.us/IEMA

INDIANA (Region V)
Mr. Patrick R. Ralston
Executive Director
Emergency Management Agency
Department of Fire and Building Public Safety
302 W. Washington Street, Room E-208
Indianapolis, IN 46204
(317) 232-3986 FAX (317) 232-3895
[redacted]@sema.state.in.us

IOWA (Region VII)
Ms. Ellen M. Gordon
Administrator
Division of Emergency Management
Hoover State Office Building, Level A
Des Moines, IA 50319-0113
(515) 281-3231 FAX (515) 281-7539
[redacted]@emd.state.ia.us
www.state.ia.us/emergency management

b6
b7C

KANSAS (Region VII)
Mr. Lloyd E. (Gene) Krase
Deputy Director
Division of Emergency Management
2800 S.W. Topeka Boulevard
Topeka, KS 66611-1287
(785) 274-1401 FAX (785) 274-1426
[redacted]@agtop.state.ks.us

KENTUCKY (Region IV)
Mr. W. R "Ronn" Padgett
Director
Division of Emergency Management
Boone Center, 100 Minuteman Parkway
Frankfort, KY 40601
(502) 607-1682 FAX (502) 607-1251
[redacted]@kydes.dma.state.ky.us
http://webserve.dma.state.ky.us

LOUISIANA (Region VI)
Colonel Michael L. Brown
Assistant Director
Office of Emergency Preparedness
P.O. Box 44217
625 N 4th Street, Basement
Baton Rouge, LA 70804
(225) 342-5470 FAX (225) 342-5471
[redacted]@hotmail.com
http://199.188.3.91

MAINE (Region I)
Mr. Bill Libby
Director
Emergency Management Agency
72 State House Station
Augusta, ME 04333-0072
(207) 626-4503 FAX (207) 626-4499
[redacted]@state.me.us

NATIONAL EMERGENCY MANAGEMENT ASSOCIATION
1999 - 2000 MEMBERSHIP ROSTER

MARYLAND (Region III)
Mr. David McMillion
Director
Emergency Management Agency
2 Sudbrook Lane, East
Pikesville, MD 21208
(410) 486-4422 FAX (410) 486-1867
(800) 636-2872
[redacted]@mema.state.md.us
www.mema.state.md.us

MASSACHUSETTS (Region I)
Mr. Stephen J. McGrail
Executive Director
Emergency Management Agency
P.O. Box 1496, 400 Worcester Road
Framingham, MA 01701
(508) 820-2010 FAX:(508) 820-2030
[redacted]@state.ma.us

MICHIGAN (Region V)
Mr. Edward Buikema
Director
Emergency Management Division
Michigan State Police
4000 Collins Road, PO Box 30636
Lansing, MI 48909-8136
(517) 333-5042 FAX (517) 333-4987
[redacted]@state.mi.us
www.mspemd.org

MINNESOTA (Region V)
Mr. Kevin Leuer
Director
Division of Emergency Management
444 Cedar Street Suite 223
St. Paul, MN 55101-6223
(651) 296-0450 FAX (651) 296-0459
[redacted]@state.mn.us
www.dps.state.mn.us/emermgt

MISSISSIPPI (Region VI)
Mr. J.E. "Jim" Maher
Director
Emergency Management Agency
P.O. Box 4501
1410 Riverside Drive
Jackson, MS 39296-4501
(601) 352-9100 FAX (601) 352-8314
[redacted]@memaorg.com
www.nemaorg.com

MISSOURI (Region VII)
Mr. Jerry B. Uhlmann
Director
Emergency Management Agency
P.O. Box 116
2302 Militia Drive
Jefferson City, MO 65102
(573) 526-9101 FAX (573) 634-7966
[redacted]@mail.state.mo.us
www.sema.state.mo.us

b6
b7C

MONTANA (Region VIII)
Mr. James F. Greene
Administrator
Disaster & Emergency Services Division
Department of Military Affairs
P.O. Box 4789
Helena, MT 59604-4789
(406) 841-3911 FAX (406) 841-3965
[redacted]@state.mt.us

NEBRASKA (Region VII)
Mr. Francis A. Laden
Assistant Director
Emergency Management Agency
1300 Military Road
Lincoln, NE 68508-1090
(402) 471-7410 FAX (402) 471-7433
[redacted]@nema.state.ne.us

NEVADA (Region IX)
Mr. Frank Siracusa
Chief
Division of Emergency Management
2525 S. Carson Street, Capitol Complex
Carson City, NV 89711
(702) 687-4240 FAX (702) 687-6788
[redacted]@quik.com

NEW HAMPSHIRE (Region I)
Mr. Woodbury P. Fogg
Director
Office of Emergency Management
State Office Park South
107 Pleasant Street
Concord, NH 03301-3809
(603) 271-2231 FAX (603) 225-7341
[redacted]@nhoem.state.nh.us

NATIONAL EMERGENCY MANAGEMENT ASSOCIATION
1999 - 2000 MEMBERSHIP ROSTER

NEW JERSEY (Region II)
Mr. Kevin Hayden
Assistant Director
New Jersey State Police
Office of Emergency Management
P.O. Box 7068, Old River Road
West Trenton, NJ 08268-0068
(609) 538-6050 FAX (609) 538-0345
[redacted]@smtp.lps.state.nj.us

NEW MEXICO (Region VI)
Mr. Ernesto Rodriguez
State Director-Emergency Management
Technical and Emergency Support Division
Department of Public Safety
P.O. Box 1628
Santa Fe, NM 87504-1628
(505) 476-9606 FAX (505) 476-9650
[redacted]@dps.state.nm.us

NEW YORK (Region II)
Mr. Edward F. Jacoby, Jr.
Director
State Emergency Management Office
1220 Washington Avenue
Building 22, Suite 101
Albany, NY 12226-2251
(518) 457-2222 FAX (518) 457-9995
[redacted]@semo.state.ny.us
www.nysemo.state.ny.us

NORTH CAROLINA (Region IV)
Mr. Eric Tolbert
Director
Division of Emergency Management
116 W. Jones Street
Raleigh, NC 27603-1335
(919) 733-3825 FAX (919) 733-5406
[redacted]@ncem.org

NORTH DAKOTA (Region VIII)
Mr. Douglas C. Friez
Director
Division of Emergency Management
P.O. Box 5511
Bismarck, ND 58506-5511
[redacted]@state.nd.us
www.state.nd.us/dem

OHIO (Region V)
Mr. James R. Williams
Executive Director
Emergency Management Agency
2855 W. Dublin Granville Road
Columbus, OH 43235-2206
(614) 889-7150 FAX (614) 889-7183
[redacted]@dps.state.oh.us

b6
b7C

OKLAHOMA (Region VI)
Mr. Albert Ashwood
Director
Department of Emergency Management
P.O. Box 53365
Oklahoma City, OK 73152
(405) 521-2481 FAX (405) 521-4053
[redacted]@oklaosf.state.ok.us

OREGON (Region X)
Ms. Myra Thompson Lee
Director
Office of Emergency Management
595 Cottage Street, N.E.
Salem, OR 97301
(503) 378-2911 FAX (503) 588-1378
[redacted]@oem.state.or.us

PENNSYLVANIA (Region III)
Mr. [redacted]
Acting Director
Emergency Management Agency
P.O. Box 3321
Harrisburg, PA 17105-3321
(717) 651-2007 FAX (717) 651-2040
[redacted]@pema.state.pa.us
www.pema.state.pa.us

PUERTO RICO (Region II)
Mr. Miguel Santini
State Director
Emergency Management Agency
P.O. Box 9066597
San Juan, PR 00906-6597
(787) 725-3234 FAX (787) 725-4244

NATIONAL EMERGENCY MANAGEMENT ASSOCIATION
1999 - 2000 MEMBERSHIP ROSTER

Mr. Ruben Rodriguez
Deputy Director
Civil Defense Agency
P.O. Box 5127
San Juan, PR 00906-6597
[redacted]

Mr. [redacted]
Operations Officer
Civil Defense Agency
P.O. Box 5127
San Juan, PR 00906-6597
[redacted] (787) 725-4244
[redacted]@prtc.net

RHODE ISLAND (Region I)
Mr. Raymond La Belle
Executive Director
Emergency Management Agency
645 London Avenue
Cranston, RI 02920
(401) 946-9996 FAX (401) 944-1891
[redacted]@ri-arng.ngb.army.mil

SOUTH CAROLINA (Region IV)
Mr. Stan M. McKinney
Director
Emergency Preparedness Division
Office of the Adjutant General
1429 Senate Street
Columbia, SC 29201
(803) 734-8020 FAX (803) 734-8062
[redacted]@strider.epd.state.sc.us

SOUTH DAKOTA (Region VIII)
Mr. John A. Berheim
Division Director
Division of Emergency Management
500 East Capitol
Pierre, SD 57501-5070
(605) 773-3231 FAX (605) 773-3580
[redacted]@state.sd.us

TENNESSEE (Region IV)
Mr. John D. White, Jr.
Director
Emergency Management Agency
3041 Sidco Drive
Nashville, TN 37204
(615) 741-4332 FAX (615) 242-9635
[redacted]@tnema.org

TEXAS (Region VI)
Mr. Tom Millwee
State Coordinator
Division of Emergency Management
Department of Public Safety
P.O. Box 4087
5805 N Lamar Blvd
Austin, TX 78773-0220
(512) 424-2443 FAX (512) 424-2444
[redacted]@txdps.state.tx.us
www.txdps.state.tx.us/dem

UTAH (Region VIII)
Mr. Earl Morris
Director
Division of Comprehensive Emergency Mgmt.
Room 1110 State Office Building
Salt Lake City, UT 84114
(801) 538-3400 FAX (801) 538-3770
[redacted]@state.ut.us
www.cem.state.ut.us/cem1.htm

VERMONT (Region I)
Mr. Ed Von Turkovich
Director
Division of Emergency Management
103 S. Main Street
Waterbury, VT 05671-2101
(802) 244-8721 FAX (802) 244-8655
[redacted]@dps.state.vt.us

VIRGIN ISLANDS (Region II)
Mr. Gene J.P. Walker
Director
Territorial Emergency Management Agency
102 Estate Hermon Hill
Christiansted, St. Croix, VI 00820
(340) 773-2244 FAX (340) 778-8980

VIRGINIA (Region III)
Mr. Michael M. Cline
State Coordinator
Department of Emergency Services
10501 Trade Court
Richmond, VA 23236
[redacted]
[redacted]@state.va.us
www.vdes.state.va.us

b6
b7C

NATIONAL EMERGENCY MANAGEMENT ASSOCIATION
1999 - 2000 MEMBERSHIP ROSTER

WASHINGTON (Region X)
Mr. Glen L. Woodbury
Director
Washington State Military Department
Emergency Management Division
Camp Murray, WA 98430
[redacted]
[redacted]@emd.wa.gov

WEST VIRGINIA (Region III)
Mr. John W. Pack, Sr.
Director
Office of Emergency Services
Main Capitol Building, Room EB-80
Charleston, WV 25305-0360
(304) 558-5380 FAX (304) 344-4538
[redacted]@wvoes.state.wv.us

WISCONSIN (Region V)
Mr. [redacted]
Administrator
Division of Emergency Management
2400 Wright Street
P.O. Box 7865
Madison, WI 53707-7865
(608) 242-3232 FAX (608) 242-3247
[redacted]@dma.state.wi.us
badger.state.wi.us/agencies/dma/em/index.htm

WYOMING (Region VIII)
Mr. Robert J. Bezek
Coordinator
Emergency Management Agency
5500 Bishop Boulevard
Cheyenne, WY 82009-3320
(307) 777-4900 FAX (307) 635-6017
[redacted]@wy-iso.army.mil

PACIFIC RIM CAUCUS

AMERICAN SAMOA (Region IX)
Mr [redacted]
TEMCO Manager
Office of the Governor
American Samoa Government
Pago Pago, AS 96799
[redacted]
(use international code 011)

GUAM (Region IX)
Mr. [redacted] b6 b7C
Acting Administrator
Department of Military Affairs
Office of Civil Defense
P.O. Box 2877
Agana, GU 96932
(671) 475-9600 FAX: (671) 477-3727
(no international code needed)

MARIANA ISLANDS (Region IX)
Mr. [redacted]
Acting Director
Emergency Management Office
Office of the Governor
Capitol Hill
P.O. Box 10007
Saipan, MP 96950
[redacted] FAX: (670) 322-1743
(no international code needed)

MARSHALL ISLANDS (Region IX)
Mr. [redacted]
Civil Defense Coordinator
Republic of the Marshall Islands
P.O. Box 15
Majuro, RMI 96960
(692) 625-3234 FAX (692) 625-3649
(use international code 011)

MICRONESIA (Region IX)
[redacted]
Special Assistant to the President for Disaster Coordination
Disaster Control
Office of the President
P.O. Box P.S. 53
Kolonia, Pohnpei, FSM 96941
(691) 320-2228 FAX (691) 320-2785
(use international code 011)

REPUBLIC OF PALAU (Region IX)
Mr. [redacted]
NEMO Coordinator
Office of the Vice President
P.O. Box 100
Koror, Republic of Palau, 96940
(680) 488-2422 FAX (680) 488-3312
(use international code 011)
nemo@palaunet.com

[rev. 8/12/1999]

National Infrastructure Protection Center
Cyber Threat and Computer Intrusion
Incident Reporting Form

This form may be used as a guide or vehicle for reporting cyber threat and computer intrusion incident information to the NIPC. The ***Cyber Incident Reporting Form*** should be submitted to your local FBI Field Office.

Report Date: _____ **Time:** _____

Point of Contact (POC) Information

Name:

Title:

Telephone/Fax number:

E-mail:

Organization:

Address or Location:

Incident Information

Name of victim:

Victim's contact information:

Telephone number:

Address:

E-mail:

Other:

Physical Location(s) of incident (Be Specific):

Purpose of System (Mission Critical):

System Status:

Date/time and duration of incident:

Nature of Problem?

Have you had this problem before? (If yes, when):

Suspected method of intrusion/attack (name of virus, name of exploit script, etc.):

The apparent source (IP address) of the intrusion/attack:

What computers/systems (hardware and software) were affected? (Operating system, version):

Do you have security Systems in place (Firewall, IDS, Banners) (Versions):

Did this intrusion/attack result in a security compromise?

Loss of classified or proprietary information?

Was there damage (physical, property damage, personal injuries, or other)?

What actions and technical mitigation have been taken so far?

Has the local FBI field office or some other agency or organization been informed?

Have you had your system prepared/replaced/updated for Y2K?

If Yes, Company/Organization who did work (Address, phone, POC information):

When was the work conducted?:

What Programs do you use? (Off the shelf, Proprietary):

If proprietary: POC for System Manager:

Who maintains your systems?: (POC information)

Any other remarks?: