U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

PUBLIC RELEASE

ASSISTANT ADMINISTRATOR FOR SATELLITE AND INFORMATION SERVICES

NESDIS Y2K Risks Are Low, But Improvements Are Needed

Inspection Report No. OSE-12199 / September 1999

Office of Systems Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
The Inspector General
Washington, D.C. 20230

September 29, 1999

MEMORANDUM FOR: Gregory W. Withee
Assistant Administrator
for Satellite and Information Services

FROM: Johnnie E. Frazier

SUBJECT: Final Inspection Report, *NESDIS Y2K Risks Are Low, But Improvements Are Needed* (Report No. OSE-12199)

The Office of Inspector General has completed a review of the National Environmental Satellite, Data, and Information Service's (NESDIS) efforts to make its computer systems year 2000 (Y2K) compliant and develop contingencies in the event that systems fail as a result of the century change. We believe that the likelihood of interruption of NESDIS satellite operations and satellite data processing due to Y2K failure is low; however, additional steps should be taken to increase confidence that failures do not occur. During the course of our evaluation and in the response to our draft report, NESDIS officials agreed to all of the recommendations in this report.

We reviewed NESDIS's renovation process for selected critical systems and concluded that the likelihood of Y2K failure is low because NESDIS exercised stringent quality control over system renovations and conducted thorough end-to-end tests. Also, because NESDIS's systems use year data infrequently, they have a low susceptibly to Y2K failures. At the same time, we are concerned that NESDIS has not completed its system inventory, which raises doubt that all systems have been evaluated for Y2K compliance. As a result, at least one system that should have been tested for compliance was not. In response to our draft report, NESDIS has re-surveyed systems in its critical business areas, updated its inventory, and evaluated the missing systems for Y2K compliance.

We also found that NESDIS needs to significantly improve and assure the accuracy of its Business Continuity and Contingency Plans (BCCPs). Although NESDIS has standard procedures for handling problems with its satellite operations and satellite data processing, the agency did not augment them with contingencies for Y2K-specific failures. NESDIS did not plan to test Y2K-specific contingencies and is instituting only limited procedures for reducing risk with computer operations for the days surrounding the century change (the Day-One plan). In response to our draft report, NESDIS has updated and corrected its BCCPs and is developing and testing Y2K contingencies. The agency also has prepared a Day-One plan.

Although NESDIS has informal procedures for managing the risk of introducing changes to operational systems, it has not established an official policy for managing changes to systems that have been confirmed to be Y2K compliant. The Office of Management and Budget (OMB) directs agencies to establish a policy limiting system changes so that Y2K compliance can be maintained. In response to our draft report, NESDIS has established formal procedures to limit system changes so that Y2K compliance can be maintained. Finally, we found several minor deficiencies in the system renovation process. In response to our draft report, NESDIS has taken additional renovation steps to increase confidence that all Y2K system problems have been found.

A copy of your full response is attached to this final report. NESDIS has a dedicated, knowledgeable staff, and we appreciate their willingness to work with us to assure that any gaps in their Y2K efforts are remedied.

BACKGROUND

NESDIS operates the National Oceanic and Atmospheric Administration's polar and geostationary environmental satellites and the Department of Defense's (DOD) polar environmental satellites. NESDIS also collects, processes, disseminates, and archives environmental data. NESDIS operates NOAA's Search and Rescue Satellite Aided Tracking system. NESDIS is a major source of weather data for the National Weather Service (NWS) and other government, commercial, and international concerns.

The Y2K problem results from computer systems that have been programmed with only the last two digits of a year rather than all four. This can cause computer systems to fail because many will not be able to distinguish between the years 1900 and 2000. Although years are infrequently used in weather data, NESDIS needs to identify and correct all Y2K defects to make sure it can provide an uninterrupted flow of data to NWS and other customers for weather forecasting and severe storm tracking.

According to NOAA's Business Continuity and Contingency Plan, NESDIS has five core business processes, three of which are critical: Satellite Operations, Satellite Data Processing, and Search and Rescue Satellite Aided Tracking. In the *NESDIS Year 2000 Item Report*, the agency identified approximately 400 application systems, operating systems, and hardware units needing Y2K consideration. Many of the systems within the three critical business processes were deemed to be mission critical.

PURPOSE AND SCOPE

The purpose of this review is to reduce the risk of critical system failure and business interruption due to the year 2000 century change by assessing actions taken by NESDIS and recommending practical Y2K risk mitigation activities. Our approach was to survey and then select a sample of

NESDIS's most critical systems and business processes to review. We assessed the renovation process for making these systems Y2K compliant and the BCCPs for the critical core business processes.

We used the *NESDIS Year 2000 Item Report* and discussions with the agency's management to select critical systems to review. Our assessment of system renovation included evaluating the extent of year usage, the thoroughness of the effort to find Y2K problems, the remediation methods, and the comprehensiveness of system testing and independent validation. We reviewed eight systems in Satellite Operations and Satellite Data Processing core business processes and performed in-depth analyses of four of them (see Appendix I). An assessment of the renovation process cannot conclusively prove that a system will be exempt from Y2K failures, but it can provide additional insight into whether the system will function properly and show whether agencies were diligent in handling Y2K problems.

We assessed NESDIS's BCCP, which consists of a matrix that identifies 30 core business sub-processes, against General Accounting Office (GAO) guidelines and performed in-depth walk-throughs of the matrix and contingency plans for Satellite Operations and Satellite Data Processing. Our BCCP work included evaluating how NESDIS managed the development of the plan and how thoroughly it analyzed the business impact of Y2K failures. We also evaluated the efficacy of NESDIS's contingency and Day-One plans and its plans for testing contingencies.

Our methodology included evaluating documentation and interviewing NESDIS staff and support contractors. Our criteria were derived from GAO and OMB guidelines for the Y2K computing crisis, research institutions, and best business practices. To ensure that needed corrections are made as quickly as possible, we kept NESDIS informed of our observations throughout our fieldwork. Our work was performed in accordance with the Inspector General Act of 1978, as amended, and the *Quality Standards for Inspections*, March 1993, issued by the President's Council on Integrity and Efficiency.

OBSERVATIONS AND CONCLUSIONS

Although NESDIS's likelihood of business interruption due to Y2K failure is low, additional measures should be taken to increase confidence that systems operate properly at the century change and that contingency plans are in place in case not all Y2K defects are identified or corrected. Specifically, the agency needs to complete its systems inventory, establish a policy for controlling changes to Y2K compliant systems, and perform additional renovation steps. Although NESDIS has standard procedures for handling problems with its satellite operations and satellite data processing, it also needs to improve its BCCPs, especially adding Y2K-specific failure scenarios and contingencies. As a result of discussions held during our fieldwork and in response to our draft report, NESDIS has agreed to all of our recommendations.

I. Rigorous System Quality Control, Thorough Testing, and Infrequent Use of Year Dates Mitigate NESDIS's Y2K Risk

NESDIS's likelihood of business interruption due to Y2K failure is low because the agency exercised rigorous quality control over system renovations and conducted thorough end-to-end tests. Also, because these systems use year data infrequently, they are less susceptible to Y2K failures.

Recognizing that it can not afford to introduce system errors that can jeopardize the continuous operation of its satellites and processing of satellite data, NESDIS has developed rigorous procedures for controlling system changes. Agencies that have sound quality control of systems changes are more likely to successfully renovate their systems for Y2K compliance. Some of the quality controls measures used by Satellite Operations and Satellite Data Processing to identify and correct system problems and move systems into operation are listed below:

- A system control board monitors the steps of the change process.
- All steps of the change process, from problem identification through testing, are documented.
- System source code is controlled using check-in and check-out library procedures.
- Tests are observed by supervisors and the originator of the change request.
- The control board approves the release of the changed system to the engineering staff.
- Engineers perform additional tests and run the new system in parallel with the production system for 10 days before putting the new system into operation.

NESDIS's experience with these quality control measures increase confidence that Y2K renovations were properly implemented.

We found that NESDIS end-to-end tests were performed in realistic operational environments, processed information for many hours, and exercised crucial year 2000 dates. This is in keeping with, for example, GAO guidance that states end-to-end tests should be run to verify that a set of interrelated systems, which collectively support a core business process, perform together as intended in an operational environment. These tests are run with times set ahead to critical dates in the year 2000 and include the exchange of data with outside organizations. NESDIS systems were part of two NWS end-to-end tests, as well as, end-to-end tests conducted within NESDIS. The NOAA geostationary satellite operations and data processing systems provided data for two 24-hour NWS end-to-end tests, one for the century rollover (December 31 to January 1) and the

other for the leap-year day (February 29 to March 1, 2000). In addition, Satellite Operations conducted one polar and three geostationary satellite end-to-end tests. These tests utilized satellites in orbit, satellites on the ground, and satellite simulators; ran for many hours; and tested the reception and dissemination of data as well as sending commands to the satellite simulator. NESDIS informed us that the tests were successful. Only minor problems were found and they were corrected. Although we did not evaluate test results, we believe that the thoroughness of these tests is a good indicator that these systems will operate properly in the year 2000.

NWS and NESDIS have stated that years are not critical to weather data or satellites. Our inspection confirmed that dates are infrequently used in the business areas we reviewed. For example, only 10 percent of Satellite Data Processing's system modules had to be renovated for Y2K compliance. Weather data is not usually dependent on years because it is short-lived and constantly updated. If dates are required, they are usually represented as a Julian date, that is, the number of days elapsed since the beginning of a year. When years are appended to weather data, they are handled properly because they usually adhere to the World Meteorological Organization standard formats for representing years. NESDIS also informed us that neither the polar nor geostationary satellites use year dates. Instead, the polar spacecraft uses a Julian date and milliseconds, which will be reset to Julian day 1 on January 1, 2000. The geostationary spacecraft uses a 24-hour clock, which is reset to zero each day. Since neither the systems we reviewed nor NOAA's geostationary or polar satellites use year data frequently, we believe that NESDIS has a low risk of Y2K failures.

At the time of our fieldwork, NESDIS systems had not been independently validated for Y2K compliance. However, Y2K tests for systems we reviewed were observed and their results confirmed by independent observers—two contractors that did not participate in system renovation. Also, critical NESDIS systems are scheduled for independent validation by the Department's independent verification and validation contractor in the near future.

II. NESDIS Inventory of Systems Should Be Updated

The *NESDIS Year 2000 Item Report* lists an inventory of approximately 400 items needing Y2K consideration. Managers use the inventory to understand the magnitude of the Y2K effort, track Y2K renovation progress, and ensure all Y2K problems have been resolved. Therefore, the inventory must be accurate and complete.

However, we found five systems missing from the inventory, including a major ground system and systems that support the polar and geostationary ground operations. The missing systems were the entire ground system for DOD's polar satellites (the Integrated Polar Acquisition and Control System); three systems within NOAA's geostationary ground operation (the Telemetry Acquisition and Command Transmission System; the Operation Ground Equipment Data Acquisition, Patching Subsystem; and the Radio Frequency equipment); and the system that handles communications between the Command and Data Acquisition station and the Satellite

Operations Control Center (the Route-About). NESDIS officials told us that one reason the systems were missing was because the contractor hired to inventory and confirm the compliance of all ground systems at the station and control center did not complete its work.

Because the inventory was incomplete, at least one system, the Telemetry Acquisition and Command Transmission System, was not tested for compliance. Although this system was part of NESDIS's geostationary satellite end-to-end test, it was not unit tested, that is, tested in isolation. After we identified this problem, Satellite Operations unit tested the system because such testing can reveal errors that are not readily detected in broader end-to-end tests.

Although we did not try to verify the completeness of business areas' system inventories, we found systems missing from the inventory in one business area as a by-product of our system review. Consequently, we are not confident that all systems within NESDIS have been identified and confirmed to be Y2K compliant. Therefore, we believe that NESDIS should re-survey systems in all five business areas to ensure that the inventory of systems for Y2K compliance review is complete. Satellite Operations has agreed to have the contractor that partially inventoried the ground systems complete the task. NESDIS's Y2K coordinator agreed to re-survey the other systems across the agency.

III. Increased Attention Should Be Paid to Business Continuity and Contingency Planning

NESDIS relies on standard procedures and the problem-solving abilities of its staff to maintain continuous operation of its satellites and processing of satellite data. NESDIS plans to deal with Y2K problems using these established procedures and consequently did not put additional effort into developing Y2K contingency plans. However, the Y2K problem is not business as usual; it has its own unique set of issues. Y2K BCCPs should identify potential business and system failures, the likelihood and impact of these failures, and contingencies to alleviate or work around them. We found the following problems with NESDIS's BCCPs: (1) lack of Y2K failure scenarios and contingencies, (2) documentation errors, (3) no plans for testing the BCCP, and (4) only limited risk mitigation activities for the days surrounding the century change (the Day-One plan). NESDIS has stated that the BCCP is a "living document" and has agreed to update it. The agency has also agreed to test Y2K contingencies where practical and is preparing a Day-One plan for the entire agency.

Lack of failure scenarios and contingencies. NESDIS did not augment its standard procedures for handling problems with its satellites and satellite data processing with Y2K failure scenarios and contingencies. Y2K-unique failures that may not be considered in normal recovery procedures include a sustained loss of externally supplied data, multiple simultaneous system failures, and a failure of both primary systems and back-ups. For example, NESDIS had not documented the possibility of a sustained failure to receive international weather data to verify NOAA polar satellite sensor readings, a possible scenario since some foreign countries are lagging behind in Y2K readiness. (After we identified this problem, NESDIS developed a

contingency plan for this failure and plans to test it.) In addition, during our interviews, NESDIS engineers identified a new contingency for circumventing a date-related failure for transmission of data from the geostationary satellite's Data Collection System. During the time of our fieldwork, Satellite Operations began drafting plans for more detailed contingencies than were presented in the BCCPs. All NESDIS business areas need to develop specific Y2K failure scenarios and contingencies using their system engineers and operators as a source of information.

Documentation errors. NESDIS should accurately document BCCPs to ensure completeness and provide confidence that adequate preparations have been made. We found one major error in its BCCP—one critical core business sub-process, DOD polar satellite ground operations, was omitted. NESDIS personnel agreed that DOD satellite operations are an important part of its mission should be addressed in the BCCP, and that the risk for NOAA satellite operations was inaccurately stated. We also identified other errors for the two business areas we reviewed including: lack of references to standard procedures, missing contingency activation criteria, lack of version control for the BCCP, duplicate business sub-processes, incorrect time when problems are anticipated to occur (should be December 31 at 7 p.m., not January 1, at midnight), and outdated risk mitigation strategies.

No plans for BCCP Y2K testing. GAO, OMB, and the President's Council on Y2K Conversion recommend that contingency plans be tested to assure that they will work if needed. Specifically, GAO guidance states that the purpose of testing is to evaluate whether Y2K contingencies provide the desired level of service to customers and can be implemented within a specified time period. However, NESDIS did not intend to test its Y2K contingency plans. One example we found where testing would be of benefit was in resolving the uncertainty of whether a particular DOD data source could be used as an alternative for polar satellite data if the latter were unavailable. We found that Satellite Data Processing did not know how long it would take to implement this contingency because it had not been used in a long time.

Risk mitigation for century change days. NESDIS is instituting only limited procedures for reducing risk with computer operations for the days surrounding the century change and has not documented these procedures in a Day-One plan. GAO guidance recommends that a Day-One plan be developed that describes the risk reduction strategy and procedures that will be used for the period between Thursday, December 30, 1999, and Monday, January 3, 2000. NESDIS has stated that personnel will be on-site on December 31 to handle systems problems and that the agency will report the status of its systems and operation to NOAA starting at 8:00 p.m., Friday, December 31. These procedures should be documented in a Day-One plan. NESDIS should also consider instituting additional activities to reduce the risks during the Day-One time period. For example, the European Meteorological Satellite Organization reported that it "is switching off

nonessential equipment during the year-end changeover" so it can focus resources on critical system.[1]

IV. An Official Policy for Managing Changes to Y2K Complaint Systems Should Be Established

Although NESDIS has procedures for managing the risk of introducing changes to operational systems, it has not established an official policy for managing changes to systems that have been confirmed to be Y2K compliant. OMB has directed agencies to establish a policy limiting system changes so that Y2K compliance can be maintained. Agencies are specifically directed to not modify systems unless absolutely necessary and to establish a process to consider the effect of the proposed changes on Y2K compliance.

NESDIS should establish policies similar to its informal procedures that reduce risk of changes. For example, NESDIS personnel do not change systems on Fridays or between December 15 and 31 because personnel may not be available on weekends or during the winter holidays. The change policy should establish a moratorium period during which only management-approved essential changes are allowed. If changes are made, they should be tested to confirm that systems remain Y2K compliant. The Federal Reserve Board, for example, is establishing a moratorium period from October 1, 1999, through March 31, 2000. Satellite Operations has agreed to consider freezing changes as of October and then re-test systems. We were recently informed by the NESDIS Y2K coordinator that the agency is writing a Y2K change policy.

V. Additional Renovation Measures Could Further Reduce Risk of System Failures

NESDIS's renovation process for the systems we reviewed was thorough. However, we found several minor deficiencies. We found that a system owner could not confirm that shared software routines that reside on Satellite Data Processing's mainframe computer were Y2K complaint. System owners should ensure that shared routines are compliant. Although Y2K compliance for most commercial products was tested, NESDIS did not test software development tools with times set ahead to critical dates in the year 2000.[2] These tools are crucial for repairing systems that fail in the year 2000.

We also found that NESDIS primarily relied on the quality control checks in the system under test and visual inspection of test results to confirm that renovated systems operated properly. However, NESDIS did not compare test results and the output of operational systems when the systems were run in parallel. Finally, although NESDIS staff performed thorough searches of

[1] "Ground Stations Could Face Y2K Problems," *Space News*, June 21, 1999, Page 14.

[2] Software development tools, such as compilers, assemblers, and linkers, are used to translate human-written programs into a format that can be executed by a computer.

systems for Y2K defects, they did not share search patterns. Many of the technical staff we interviewed agreed that additional renovation measures would be beneficial.

CONCLUSION AND RECOMMENDATIONS

We believe the likelihood of interruption of NESDIS's satellite operations and satellite data processing due to Y2K failure is low; however, additional steps should be taken to increase confidence that failures do not occur. Throughout our fieldwork, agency staff have agreed to take the actions cited in this report. Although our evaluation was limited to the most critical systems and business processes, our recommendations apply to all NESDIS's business areas.

We recommend that the Assistant Administrator for Satellite and Information Services direct the NESDIS staff to take the following actions:

1. Complete its system inventory:
   a. Re-survey systems in all business areas, and
   b. Confirm that any new systems found are Y2K compliant.

2. Update all of NESDIS's Business Contingency and Continuity Plans to ensure that:
   a. Y2K-specific failure scenarios and contingencies are developed,
   b. Documentation errors are corrected,
   c. Existing and newly developed contingencies are tested, and
   d. NESDIS's Day-One plan is completed.

3. Establish a NESDIS-wide policy for changes to Y2K compliant systems that includes:
   a. Effective time frames,
   b. Procedures for evaluating proposed changes, and
   c. If changes are needed, the re-testing required to assure Y2K compliance is maintained.

4. Perform the following additional renovation steps for all of NESDIS's systems:
   a. Confirm compliance of shared code,
   b. Test compliance of system development tools,
   c. Compare test result with operational results, if available, and
   d. Search systems for Y2K defects if new search patterns are found among the staff.

NESDIS has agreed with all of our recommendations. The agency has taken or plans to take actions that are responsive to our recommendations.

Appendix I

NESDIS Systems Reviewed

We reviewed eight critical system in two of NESDIS's most important business processes. Within Satellite Operations, we reviewed three systems that are part of ground operations for the two NOAA environmental satellites—Geostationary Operational Environmental Satellite (GOES) and the Polar-orbiting Operational Environmental Satellite (POES):

- OATS— Orbital Attitude and Tracking System .
- GIMTACS—GOES I through M Telemetry and Command System.
- PACS— Polar Acquisition and Control System.

We reviewed five systems in Satellite Data Processing that processed four weather data products:

- Environmental product system.
- Shared processing products system.
- GOES winds and imagery product systems.
- RTOVS—Replacement Trios Operational Vertical Sounder (for NOAA's older polar satellites).
- ATOVS—Advanced Trios Operational Vertical Sounder (for NOAA's new polar satellite NOAA-15).

Attachment

SEP 27 1999

UNITED STATES DEPARTMENT OF COMMERCE
National Oceanic and Atmospheric Administration
CHIEF FINANCIAL OFFICER/CHIEF ADMINISTRATIVE OFFICER

MEMORANDUM FOR: Judith J. Gordon
Assistant Inspector General for
Systems Evaluation

FROM: Paul F. Roberts Barbara Mantini (for)

SUBJECT: Response to Office of Inspector General (OIG) Draft Inspection Report, NESDIS Y2K Risks are Low, But Improvements Are Needed
Report No. OSE-12199

Thank you for the opportunity to review and comment on the subject OIG draft inspection report. We agree with your conclusion that the likelihood of interruption of the NESDIS Satellite Operations and Satellite Processing due to Y2K failures is low. The NESDIS Y2K failure rate is low because our systems use year dates infrequently; we exercised stringent configuration management control over system renovations; and we conducted thorough end-to-end tests. However, we also agree with your findings that additional steps should be taken to increase confidence that Y2K failures do not occur. In response to your observations and recommendations, the National Satellite, Data, and Information Service has completed the following actions.

1. **Office of Inspector General Recommendation:** Complete system inventory:

   a. Re-survey systems in all business areas, and
   b. Confirm that any new systems found are Y2K compliant.

Actions Taken or Planned: NESDIS has re-surveyed systems in mission critical areas to ensure that the NESDIS Y2K database is accurate and complete. This action resulted in the addition of seven subsystems to the Y2K database. The Integrated Polar Acquisition Control System (IPACS) ground system was not in our Y2K database initially because it was still under development by the Office of Systems Development during our evaluation. Six records have been added to the Y2K database to include all components of the IPACS. The contractor was required to develop and deliver the IPACS system as Y2K compliant. National Oceanic

Printed on Recycled Paper

and Atmospheric Administration (NOAA) and Air Force personnel were present when the Y2K compliance tests were conducted by the contractor. We have also added the Telemetry and Command Transmission System to the database. The source code has been evaluated, and use of year dates was minimal. This system has been confirmed as Y2K compliant.

During your review of Satellite Operations, the following components were also identified; however, they have not been added to the Y2K database since they are subsystems of other systems already listed in the Y2K database. The Operational Ground Equipment Data Acquisition, Patching Subsystem consists of patch panels, demodulators, and bit synchronizers that have no software and no date-time dependencies or even any means of inputting a date or time. This was used in all of the Satellite Operations Geostationary Operational Environmental Satellite end-to-end simulations and is part of the GOES I through M Telemetry and Command System (GIMTACS) ground system hardware.

The RouteAbouts are bridging routers which have no software and no date or time except for use in time tagging log messages. This feature is disabled since it provides only delta time from the last reset of the RouteAbout and is of little practical value. Therefore, the time is not even set on these devices. The RouteAbouts were certified compliant by the vendor and have been used in all of our end-to-end tests. These hardware devices are used by GIMTACS, PACS, and IPACS. All of the above actions were completed on September 3, 1999.

2. **Office of Inspector General Recommendation:** Update all of NESDIS's Business Contingency and Continuity Plans (BCCP's) to ensure that:

   a. Y2K-specific failure scenarios and contingencies are developed,
   b. Documentation errors are corrected,
   c. Existing and newly developed contingencies are tested, and;
   d. NESDIS's Day-One Plan is completed.

Action Taken or Planned: NESDIS reviewed our BCCP and corrected documentation errors on August 4, 1999. In addition, the BCCP was updated to include one critical core business sub-process,

references to standard operating procedures, and contingency activation criteria. This task was completed on September 8, 1999.

NESDIS has made significant progress in developing Y2K contingencies and testing our BCCP. NESDIS representatives participated in the two BCCP workshops held during August by the Department of Commerce (DOC). Specific Y2K business and system failures were documented and contingencies to alleviate them were developed. In addition, the backup power generators and telecommunications systems are tested routinely.

At the direction of DOC, NESDIS has developed a Day-One Plan. The plan identifies an architecture for Day-One activities for NESDIS's mission critical systems, telecommunications, and facilities. This plan was developed and submitted to the NOAA Y2K coordinator for review on August 31, 1999. On September 9, 1999, NESDIS staff participated in the NOAA Day-One Plan workshop with the other NOAA line offices.

3. **Office of Inspector General Recommendation:** Establish a NESDIS-wide policy for changes to Y2K compliant systems that includes:

   a. Effective time frames,
   b. Procedures for evaluating proposed changes, and
   c. If changes are needed, the re-testing required to assure Y2K compliance is maintained.

Action Taken or Planned: NESDIS has established formal procedures to limit system changes so that Y2K compliance can be maintained. As part of standard operating procedures, NESDIS has implemented a rigorous configuration management system for controlling system changes. Each mission critical system has established a moratorium period for system changes and a waiver process if changes are essential. If changes are necessary, they will be tested using the configuration management process to ensure Y2K disruptions do not occur. NESDIS is experienced with handling year end rollovers, and annually establishes change policies for all systems. This task was completed on September 8, 1999.

4. **Office of Inspector General Recommendation:** Perform the following additional renovation steps for all of NESDIS's systems:

   a. Confirm compliance of shared code,
   b. Test compliance of system development tools,
   c. Compare test result with operational results, if available, and
   d. Search systems for Y2K defects if new search patterns are found among the staff.

Actions Taken or Planned: NESDIS confirmed the Y2K compliance of all shared code in March 1999. All software development tools, such as compilers, assemblers, and linkers have been verified as Y2K compliant. All systems have been thoroughly searched using the same search patterns. This task was completed on September 8, 1999.