

U.S. DEPARTMENT OF COMMERCE
Office of Inspector General



**PUBLIC
RELEASE**

*NATIONAL OCEANIC AND
ATMOSPHERIC ADMINISTRATION*

*NWS Y2K Risks Are Low
and Agency Is Well Prepared*

Inspection Report No. OSE-12313 / December 1999

Office of Systems Evaluation





December 6, 1999

MEMORANDUM FOR: John J. Kelly, Jr.
Assistant Administrator for Weather Services

FROM: 
Johnnie E. Frazier

SUBJECT: Final Inspection Report, *NWS Y2K Risks Are Low and Agency Is Well Prepared* (Report No. OSE-12313)

The Office of Inspector General has completed a review of the National Weather Service's efforts to reduce the risk of business interruption due to the year 2000 (Y2K) century change. We believe that the likelihood of interruption of NWS operations due to Y2K failure is low, with the exception of the possible loss of international weather data from countries that are at risk for Y2K failures. However, NWS has developed contingencies to compensate for the loss of this data. We did not review the Y2K compliance of NWS's eight national mission critical systems because they were being evaluated by the Department's Y2K validation contractor.¹

Because we did not find any significant weaknesses in the aspects of the NWS Y2K program that we reviewed, we have not made any recommendations and are issuing this report in final. We would like to thank the dedicated and knowledgeable staff of NWS for working with us to complete this review.

BACKGROUND

NWS provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters, and ocean areas for the protection of life and property and the enhancement of the national economy. NWS data and products form a national information database and infrastructure that can be used by other governmental agencies, the private sector, the public, and the global community. NWS provides warnings and forecasts of hazardous weather, including thunderstorms, flooding, hurricanes, tornadoes, winter weather, tsunamis, and

¹The following eight national systems were identified by the NWS as most critical to its operations: (1) Automated Surface Observing System (ASOS), (2) Next Generation Weather Radar (NEXRAD), (3) Advanced Weather Interactive Processing System (AWIPS), (4) NWS Telecommunication Gateway (NWSTG), (5) National Centers for Environmental Prediction (NCEP), (6) NWS Upper-Air program, (7) NWS River Forecast System (NWSRFS), and (8) Automation of Field Operations and Services (AFOS).

climate events. The NWS is the United States' sole official voice for issuing warnings during life-threatening weather situations.²

The Office of Management and Budget has identified NWS as a Y2K high impact federal agency because of the importance of its services to the public. 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 approach 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, NWS needs to identify and correct all Y2K defects to make sure it can provide forecasts and warnings without interruption.

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 NWS and, if appropriate, recommending practical Y2K risk mitigation activities. We reviewed five aspects of the NWS Y2K program: (1) business continuity and contingency planning, (2) NWS end-to-end tests, (3) external data exchanges, (4) policies for maintaining Y2K compliance, and (5) the compliance of systems used to notify the public of weather conditions. We did not review the Y2K compliance of NWS's eight national mission critical systems because they were being evaluated by the Department's Y2K validation contractor.

Our methodology included evaluating documentation and interviewing NWS staff involved in the Y2K effort. Our criteria were derived from GAO and OMB guidelines for the Y2K computing crisis, research institutions, and best practices. 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. We conducted our fieldwork between August and November 1999.

OBSERVATIONS AND CONCLUSIONS

NWS Y2K Risks Are Low and Agency Is Well Prepared

We found three factors that significantly reduce the likelihood of Y2K-induced interruption of NWS operations. First, NWS systems have a low susceptibility to Y2K failures because weather systems use year data infrequently. NWS estimates that five percent or less of its data contains year information. Second, NWS has experience using its well-documented, in-depth contingency plans for maintaining continuous operations. For example, in September 1999, NWS was able to recover from a catastrophic loss of its supercomputer, which is fundamental to weather

²National Weather Service Strategic Plan for Weather, Water, and Climate Services, 2000 - 2005, August 1999.

forecasting. Third, NWS has adequately tested its ability to receive and send weather data internally and with data exchange partners, which is crucial to generating and distributing forecasts. This ability was demonstrated in two Y2K end-to-end tests, which included participation by governmental, private, and international concerns.

In the remaining areas of our review we also found that NWS was Y2K-ready. Its external data exchanges, like other weather data, use year data infrequently. NWS tested external data exchanges in the Y2K end-to-end tests and reported problems were corrected. We found that although NWS does not have an official policy for freezing or regulating changes to compliant systems, it does not plan to upgrade its eight national mission critical systems before the end of the year. Upgrades that have occurred have gone through a process that ensures that systems were re-tested for Y2K compliance. Finally, four systems NWS uses to notify the public of severe weather conditions have been confirmed to be compliant.³

We believe that NWS's greatest Y2K risk is the possible loss of international weather data from countries that are at risk for Y2K failures. However, NWS has developed contingencies, including alternate data transmission paths and data sources, to compensate for the loss of this data. In the worst case, NWS meteorologists would rely on data from local, ground-based observations and satellite data products to produce forecasts and severe weather warnings.

³The following four systems are used to notify the public of weather conditions: (1) NOAA Weather Wire Service (NWWS) satellite uplink system, (2) NOAA Weather Radio (NWR) broadcast system and its associated digital Console Replacement System (CRS), (3) NEXRAD Information Distribution Service (NIDS) which is part of the NEXRAD system, and (4) Emergency Managers Weather Information Network (EMWIN).