



# Report In Brief

U.S. Department of Commerce, Office of Inspector General

December 2009



## Why We Did This Review

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to identify and provide security protection of information collected or maintained by them or on their behalf. Inspectors general are required to annually evaluate agencies' information security programs and practices. Such evaluations must include testing of a representative subset of systems and an assessment, based on that testing, of the entity's compliance with FISMA and applicable requirements.

This review covers our evaluation of NOAA's ESPC, which is one of a sample of systems we assessed in FY 2009.

## Background

ESPC is NOAA's primary processing system for the nation's environmental satellite data. ESPC ingests, processes, distributes, and archives data from two environmental and meteorological satellite systems.

C&A is a process by which security controls for IT systems are assessed to determine their overall effectiveness. Understanding the remaining vulnerabilities identified during the assessment is essential in determining the risk to the organization's operations and assets, to individuals, to other organizations, and to the national resulting from the use of the system. Continuous monitoring is a critical post-accreditation aspect of this process.

## National Oceanic and Atmospheric Administration (NOAA)

### *FY 2009 FISMA Assessment of the Environmental Satellite Processing Center (ESPC) (OAE-19730)*

## What We Found

Our objectives for this review were to determine whether (1) implemented controls adequately protected the system and its information, (2) continuous monitoring is keeping the authorizing official sufficiently informed about the operational status and effectiveness of security controls, and (3) the certification and accreditation (C&A) process produced sufficient information about remaining system vulnerabilities to enable the authorizing official to make a credible, risk-based accreditation decision.

We found that the National Environmental Satellite, Data, and Information Service has not followed the required process for C&A of ESPC. The lack of proper security planning undermined the effectiveness of the system's security certification, hindering the authorizing official in making a credible risk-based accreditation decision. The system's plan of action and milestones for remediating vulnerabilities is ineffective.

## What We Recommend

We recommend that NOAA complete security planning activities, conduct appropriate security control assessments, and address system deficiencies. Until these activities have been completed, NOAA should revise the system's accreditation status to an interim authorization to operate.

In its response to our draft report, NOAA disputed our findings and concurred with only two of our recommendations. NOAA does agree that ESPC's security posture must improve. We have asked NOAA to reconsider its response based on our comments in this report and craft its action plan, due in 60 days, accordingly.