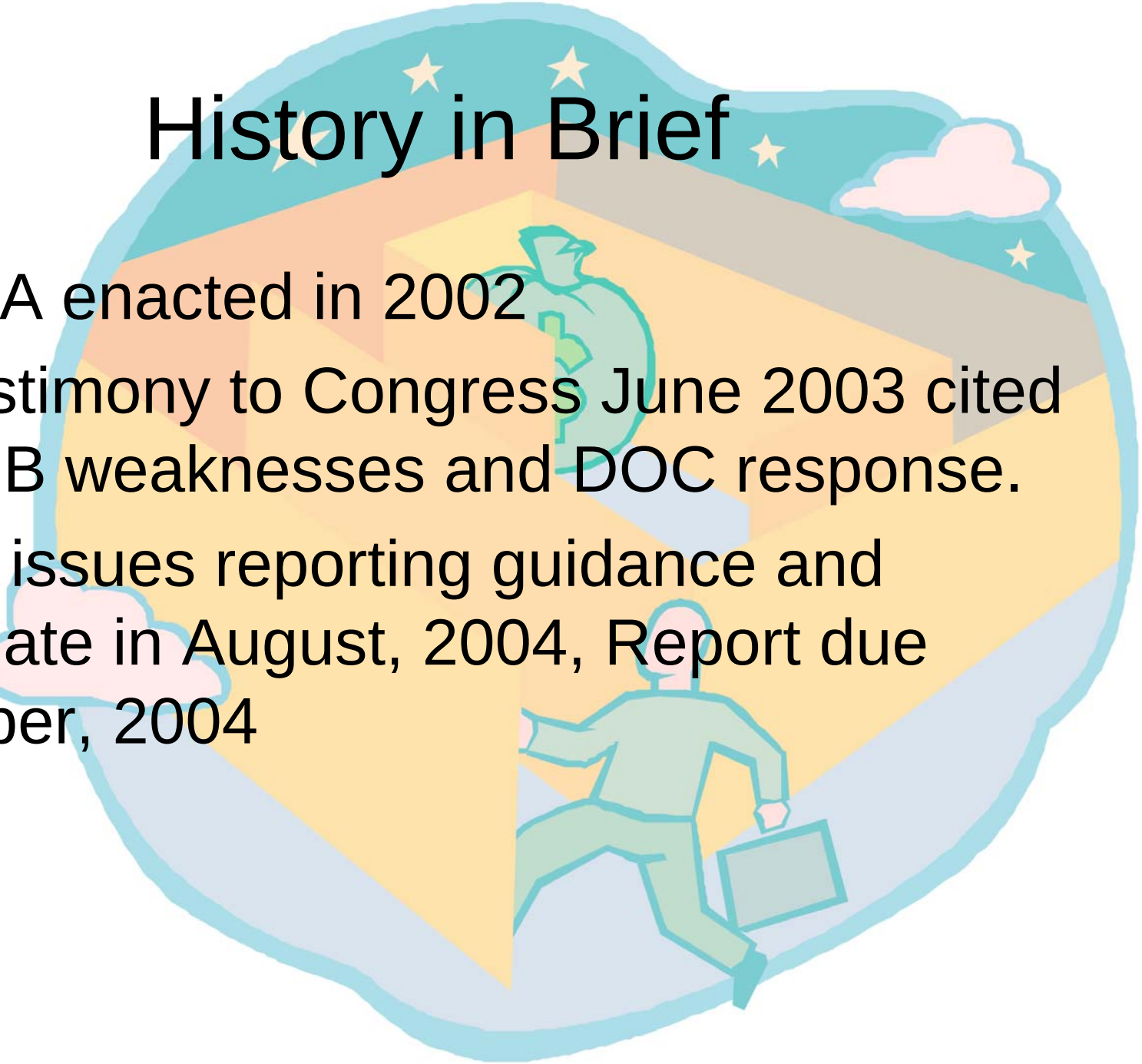
ACSAC
NOAA/NESDIS Case Study

December, 2006

History in Brief



- FISMA enacted in 2002
- IG testimony to Congress June 2003 cited 6 OMB weaknesses and DOC response.
- OMB issues reporting guidance and template in August, 2004, Report due October, 2004

OMB 2004 report to congress on Implementation of FISMA

March 2005, Initial FISMA report to Congress

DOC IG report:

Quality of C&A process – Poor

U.S. DOC OIG

Top Ten Management Challenges, March 2005

- Departmental Material Weakness in Performance and Accountability Report for previous 4 years.
- OIG concluded that there were problems with conduct of Assessing risk, identifying the system components, and testing security controls.
- CIO issued a plan to correct the material weakness including establishing repeatable processes that produce acceptable packages.

OMB 2005 report to congress on Implementation of FISMA

Again Cites DOC IG report:

Quality of C&A process – Poor

U.S. DOC OIG

Top Ten Management Challenges, Sept 2005

- NOAA had significantly improved risk assessments, security plans, and testing.
- OIG concluded that the C&A process did not provide adequate vulnerability data to the AO at time of decision.

US DOC OIG

Top Ten Management Challenges, March 2006

- Sept 2005 Findings Presented to December 2005 CIO Meeting.

OMB 2006 report to congress on Implementation of FISMA

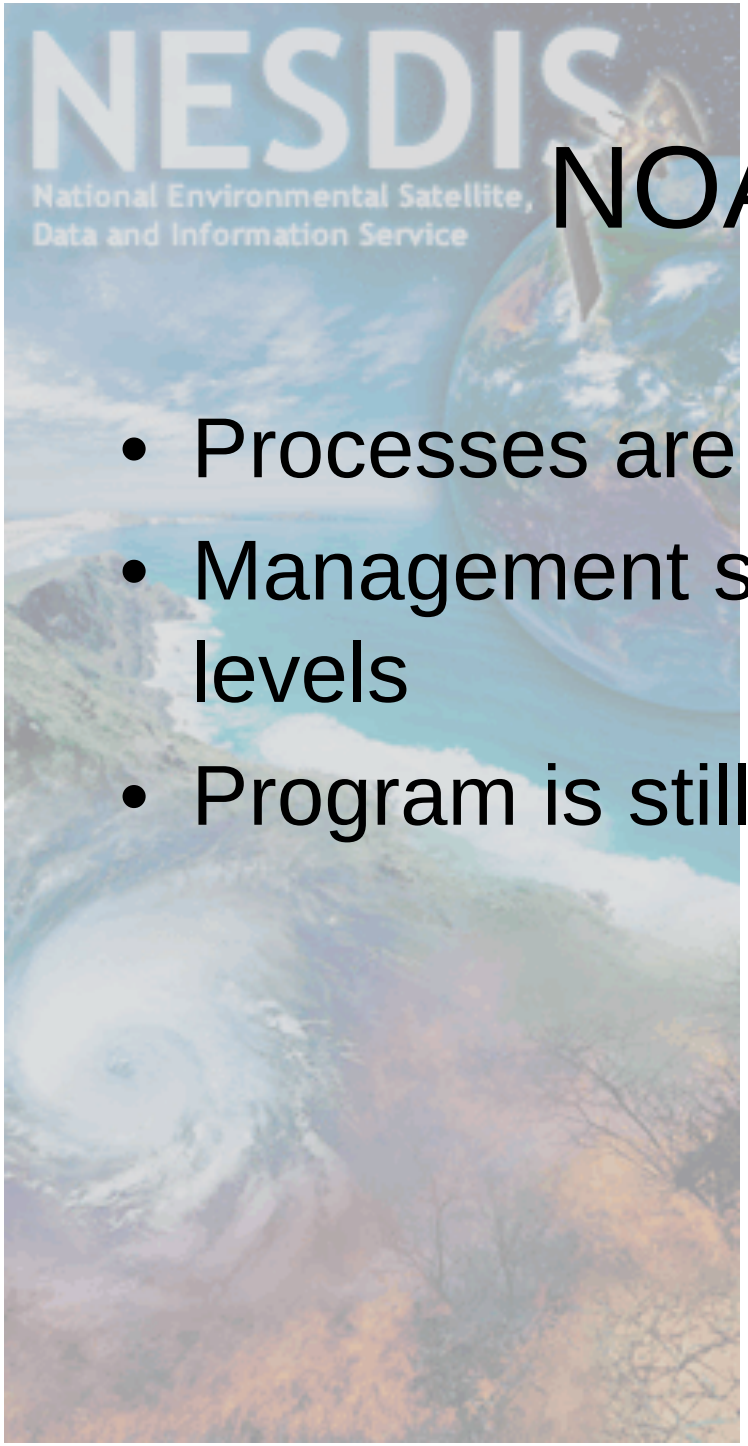
Cites DOC IG report:

Quality of C&A process – Showed significant improvements

- NOAA had significantly improved risk assessments, security plans, and testing.
- OIG concluded that the C&A process still did not provide adequate vulnerability data to the AO at time of decision.

Summation of Status

- Security was a significant problem through 2004.
- Processes put into place by the CIO to correct the deficiencies.
- Processes need improvement in identified areas.
- OIG September 2006 report not yet released to public.



NOAA/NESDIS

- Processes are in-place and improving
- Management support excellent at higher levels
- Program is still expensive and complex.

Processes are in place

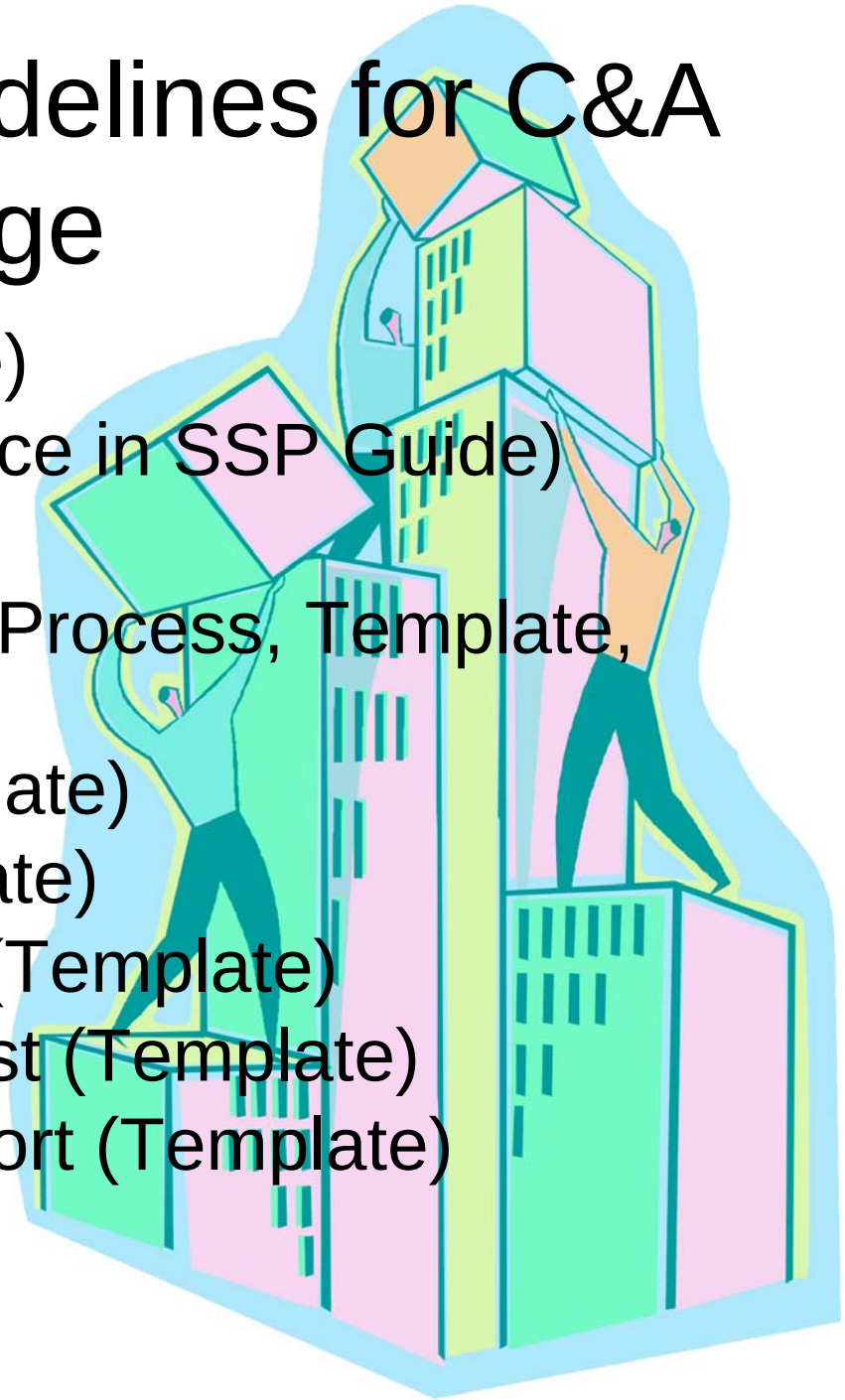
- Standardized schedule for C&A
- Templates and guidelines for C&A package updated for SP 800-53 Controls
- Risk Assessment to include vulnerability and control testing results
- Testing Updated to SP 800-53A

Standardized Schedule for C&A

- Addresses events from initial meeting to signing of the approval.
- Has undergone significant upgrade over two years of experience
- Incorporates QA reviews, management reviews
- Portrays a 9 month Legacy process assuming everyone delivers on schedule

Templates and Guidelines for C&A package

- SSP (Template and Guide)
- System Topology (Guidance in SSP Guide)
- MOU/A or ISA (Template)
- Risk Assessment Report (Process, Template, Guide)
- Test Reports (Plan, Template)
- Contingency Plan (Template)
- Contingency Test Report (Template)
- Certification Validation Test (Template)
- Security Assessment Report (Template)



Risk Assessment

Multiple Pass Process defined.

Facilitate Risk Assessment

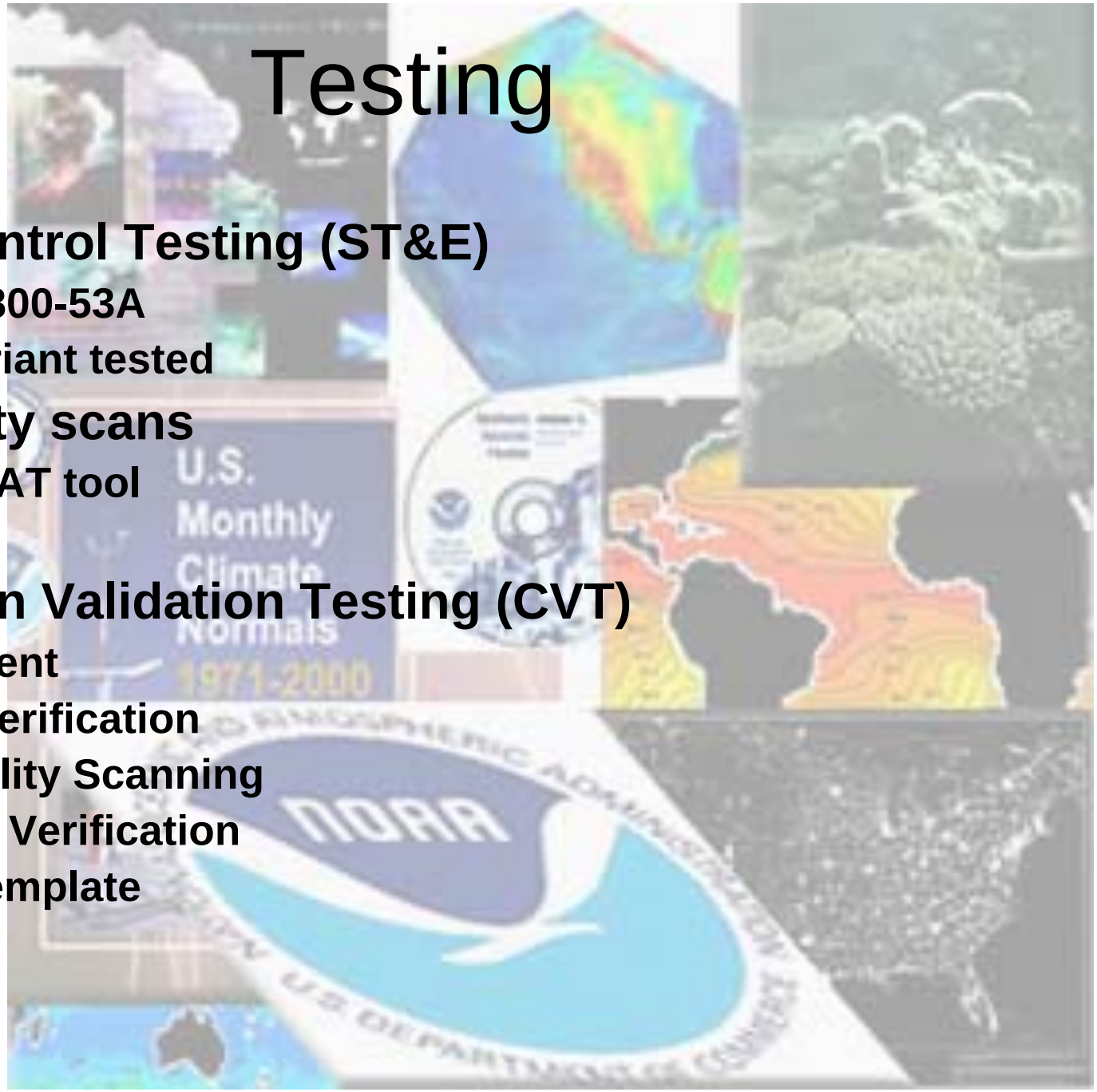
Scan Vulnerabilities

Internal ST&E

(Penetration Testing)

POA&M Maintained

Testing



- **Internal Control Testing (ST&E)**
  - **NIST SP 800-53A**
  - **Every Variant tested**
- **Vulnerability scans**
  - **Harris STAT tool**
  - **Nesses**
- **Certification Validation Testing (CVT)**
  - **Independent**
  - **Control Verification**
  - **Vulnerability Scanning**
  - **Inventory Verification**
  - **Report Template**

Key Constraints

- Strict Conformance to NIST guidelines
- Inventory, topology and scans must totally match
- System descriptions must explain each component in logical sequence.
- Full FIPS 199 Information analysis
- Personal Information Assessment

Submission

Security Assessment Report to AO

- Every vulnerability must have risk assessment and POA&M
- Summarizes package.
- Template

Conclusion

NOAA/NESDIS has significantly improved the process under FISMA by using NIST SP guidance and DOC OIG comments to improve the process.