FISMA

Yesterday, Today, Tomorrow

Tammy L. Whitcomb
Acting Inspector General
U.S. Postal Service

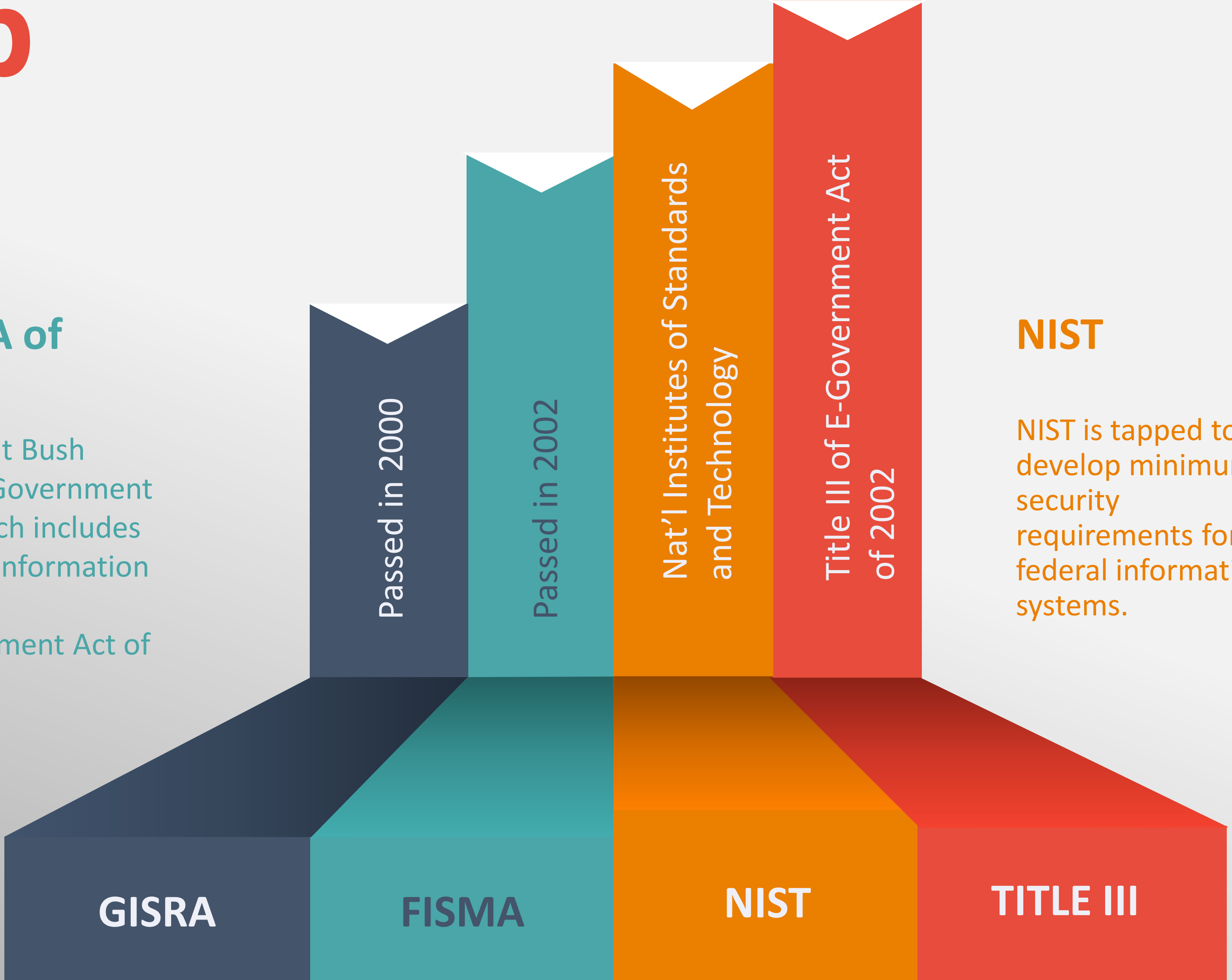
Laws Start to Catch Up

GISRA of 2000

The Government Information Security Reform Act (GISRA) of 2000 provided a framework to strengthen information security requirements.

FISMA of 2002

President Bush signs E-Government Act, which includes Federal Information Security Management Act of 2002.



Passed in 2000

Passed in 2002

Nat’l Institutes of Standards and Technology

Title III of E-Government Act of 2002

GISRA

FISMA

NIST

TITLE III

NIST

NIST is tapped to develop minimum security requirements for federal information systems.

Title III

FISMA is Title III of the E-Government Act of 2002, which required each federal agency to develop, document, and implement agency-wide program. IGs would perform annual independent evaluation.

FISMA 2002: Info Security Domains

- Info Security Continuous Monitoring
- Configuration Management
- Identity and Access Mgmt
- Risk Management
- Contractor Systems

Reporting guidance focused on yes/no questions

- Incident Response and Reporting
- Security Training
- Plan of Action and Milestones
- Contingency Planning

Effectiveness v. Compliance

IGs assess the effectiveness of agency information security programs by addressing extent to which controls are implemented correctly, operating as intended, and producing desired outcome.

Working in Consultation

OMB, in consultation with DHS, the Chief Information Officers Council, and CIGIE develop guidance for evaluating the effectiveness of information security programs and practices.

Maturity Model

Decision was made to transition the IG FISM A metrics to a maturity model approach, which would provide a better view into the status of information security programs.

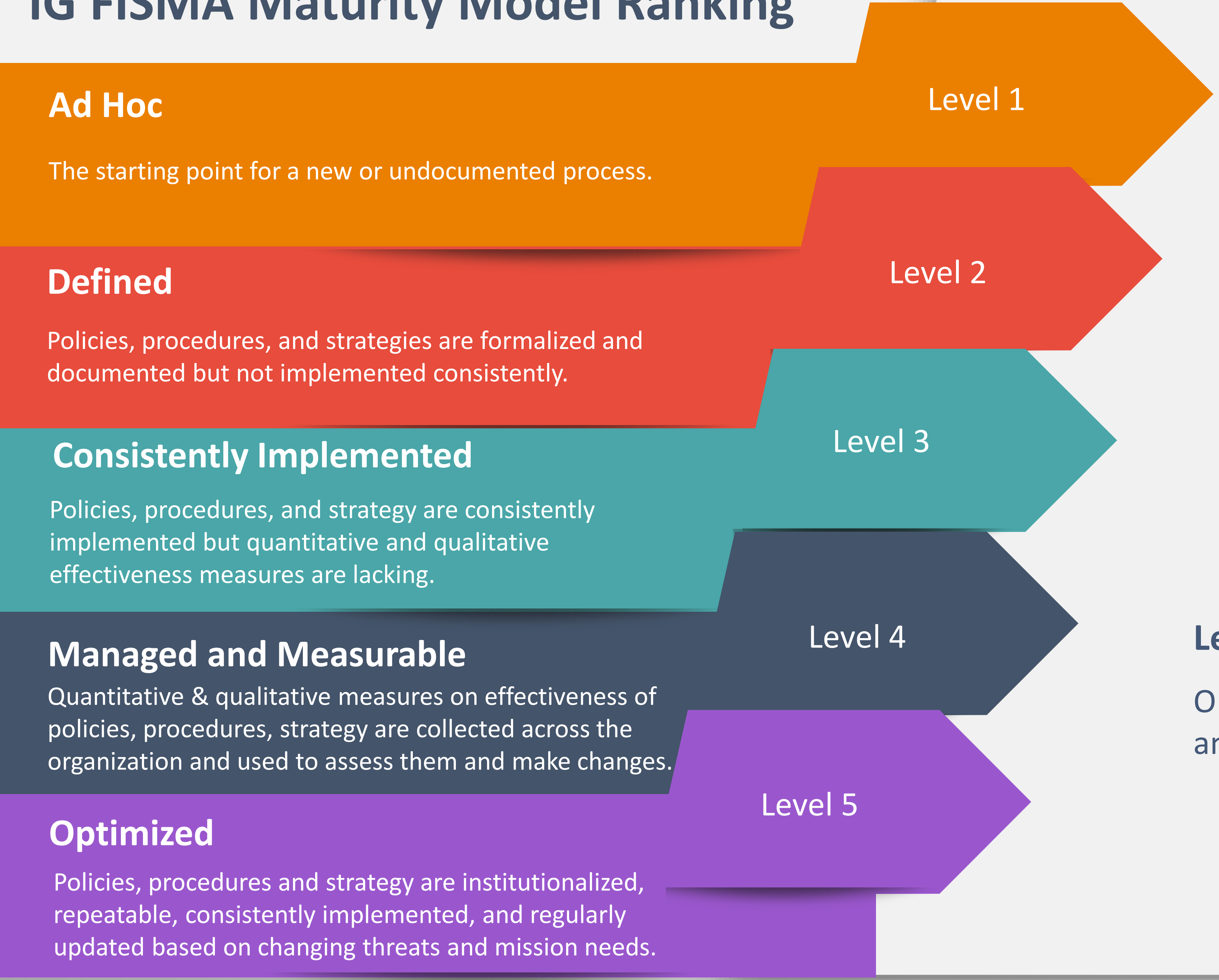
Continuous Improvement

Maturity is a measurement of the ability of an organization for continuous improvement in a particular discipline.

FISMA Modernization Act

In 2014, the FISMA Modernization Act of was passed to strengthen the information security requirements of FISMA of 2002. The updated Act moved away from measuring compliance to measuring effectiveness.

IG FISMA Maturity Model Ranking



Level 1

Ad Hoc

The starting point for a new or undocumented process.

Level 2

Defined

Policies, procedures, and strategies are formalized and documented but not implemented consistently.

Level 3

Consistently Implemented

Policies, procedures, and strategy are consistently implemented but quantitative and qualitative effectiveness measures are lacking.

Level 4

Managed and Measurable

Quantitative & qualitative measures on effectiveness of policies, procedures, strategy are collected across the organization and used to assess them and make changes.

Level 5

Optimized

Policies, procedures and strategy are institutionalized, repeatable, consistently implemented, and regularly updated based on changing threats and mission needs.

Level 4

OMB has designated Level 4 as the bar for an effective program.

2015 ISCM Evaluation Results

Agency Progress Against ISCM CAP Goals	
Automated Software Asset Inventory	89%
Capability to Detect & Block Unauthorized Software	68%
Secure Configuration Management	92%
Vulnerability Management	52%

≠

OIG ISCM Maturity Evaluations

Maturity Level	No. of Agencies	%
Ad Hoc	15	63%
Defined	6	25%
Consistently Implemented	2	8%
Managed and Measurable	0	0%
Optimized	0	0%
Not Scored	1	4%

Source: OMB FY 2016 FISMA Report to Congress

NEXT STEPS

Improve evaluation guide

Keep Building

Detailed test steps for IG evaluators to utilize, questions to ask, things to look for, particularly at higher levels of maturity.

More robust scoring methodology

Incorporate

Weighting applied to attributes that are of greater risk or concern to stakeholders.

Tailor maturity attributes

Evaluate Options

Tailor maturity attributes based on organizational missions/resources/risks.