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

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

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

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

Effectiveness vs. 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.

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

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

Consistently Implemented
Policies, procedures, and strategy are consistently implemented but not implemented consistently.

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

Ad Hoc
The starting point for a new or undocumented process.

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated Software Asset Inventory</td>
<td>89%</td>
</tr>
<tr>
<td>Capability to Detect &amp; Block Unauthorized Software</td>
<td>68%</td>
</tr>
<tr>
<td>Secure Configuration Management</td>
<td>92%</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>52%</td>
</tr>
</tbody>
</table>

OIG ISCM Maturity Evaluations

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>No. of Agencies</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad Hoc</td>
<td>15</td>
<td>63%</td>
</tr>
<tr>
<td>Defined</td>
<td>6</td>
<td>25%</td>
</tr>
<tr>
<td>Consistently Implemented</td>
<td>2</td>
<td>8%</td>
</tr>
<tr>
<td>Managed and Measurable</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Optimized</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Not Scored</td>
<td>1</td>
<td>4%</td>
</tr>
</tbody>
</table>
Detailed test steps for IG evaluators to utilize, questions to ask, things to look for, particularly at higher levels of maturity.

Keep Building

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

Evaluate Options

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

Incorporate

More robust scoring methodology

Improve evaluation guide

NEXT STEPS