FISMA – Perspectives from OMB and DHS

Federal Network Resilience, Cybersecurity Performance Management
Updated: June 11, 2013

Homeland Security

For Official Use Only

OMB Memorandum M-10-28

- Outlines and clarifies the respective responsibilities and activities of the Office of Management and Budget (OMB), the Cybersecurity Coordinator, and the Department of Homeland Security, in particular with respect to the Federal Government's implementation of the Federal Information Security Management Act of 2002.

Homeland Security

OMB 10-28 Activities and Responsibilities

- DHS will:
  - oversee reporting on cybersecurity policies and guidance;
  - oversee efforts to provide adequate, risk-based and cost-effective cybersecurity;
  - oversee compliance with FISMA and develop analyses for OMB to assist in the development of the FISMA annual report;
  - oversee the agencies' cybersecurity operations and incident response and providing appropriate assistance; and
  - annually review the agencies' cybersecurity programs.

CPM Reporting and Trending

- As required by FISMA, OMB must report on the FISMA Results of each agency
- FNR Cybersecrity Performance Management (CPM) is the Analytics team that develops, collects, and analyzes all agency reporting information.
- CPM reports all Administrative Priority Metrics for each agency to OMB on a quarterly basis.
- CPM assists OMB with the annual FISMA congressional Report.

How does FISMA guidance gets created?

- DHS provides operational guidance, working in concert with OMB on enterprise management.
- DHS, through FNR, effects policy implementation through FISMs - objectively developed interagency governance that uses a collaborative, consolatory approach.
- Progress is measured through statistical sampling of agencies using consistent, quantitative measures.
- These metrics help to ensure FNR effects informed, risk-based decisions to continue to establish governance with the purpose of driving measurable progress and outcomes.

Homeland Security

Metrics

- Metrics are classified into three categories:
  - Administration Priorities (AP)
  - Key FISMA Metrics (KFM)
  - Baseline (BASE).
- The AP metrics highlight three areas:
  - Trusted Internet Connection (TIC)
  - Personal Identity Verification (PIV) mandatory authentication with Personal Identity Verification
  - Continuous Monitoring.
- Key metrics are the additional metrics outside of the Administration priorities that are measured (scored). Baseline FISMA metrics are not scored, but used to establish current baselines against which future performance may be measured.

Homeland Security

Guidance

- Metrics and Guidance are subject to continuous improvement
  - Over 250 resource hrs. to-date responding to community feedback regarding FY14 CIO metrics
  - Active working group with members of the IG community on development of FY14 IG metrics
  - FY14 metric development is significantly ahead of last years schedule
- New in FY13, each metric is scored for impact (significance, relevance, reliability, clarity, impact)
- DHS is committed to developing guidance with the user in mind. Guidance is developed to help the user:
  - find what they need,
  - understand what they find; and
  - use what they find to meet their needs.

Homeland Security

Dave Otto
Branch Chief, Cybersecurity Performance Management
Department of Homeland Security
Federal Network Resilience
Desk: 703-235-4945
Email: david.otto@dhs.gov

Homeland Security