FISMA – FY15 CIO Metrics

DHS Federal Network Resilience
Updated: August 19, 2014

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

Pursuant to OMB M-10-28

- 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

Homeland Security

Collection & Reporting

- Pursuant to 44 U.S.C. § 3544, OMB must report on the FISMA Results of each agency
- DHS, Federal Network Resilience, Cybersecurity Performance Management Branch (CPM) is the functional team that develops, collects, and analyzes all agency reporting information for the OMB report
- In accordance with the Government Performance and Results Modernization Act (P.L. 111-352), CPM collects and reports on Administration Priority (AP) metrics on a quarterly basis
- CPM provides an array of customers with ad hoc analysis and reporting

Homeland Security

FY15 FISMA CIO Metric Development Process

- Agile Sprint approach utilizing an interactive webinar
- Engaged 22 CFO Act Departments and Agencies
- Adjudicated feedback on the entire catalog of metrics
- Feedback has resulted in significant improvements in clarity and readability
- Achieved 18% reduction in metric count despite adding 41 new metrics to reflect new CAP goal requirement
- Community members engaged in final quality review to identify issues and defects found in the Release Candidate

Homeland Security

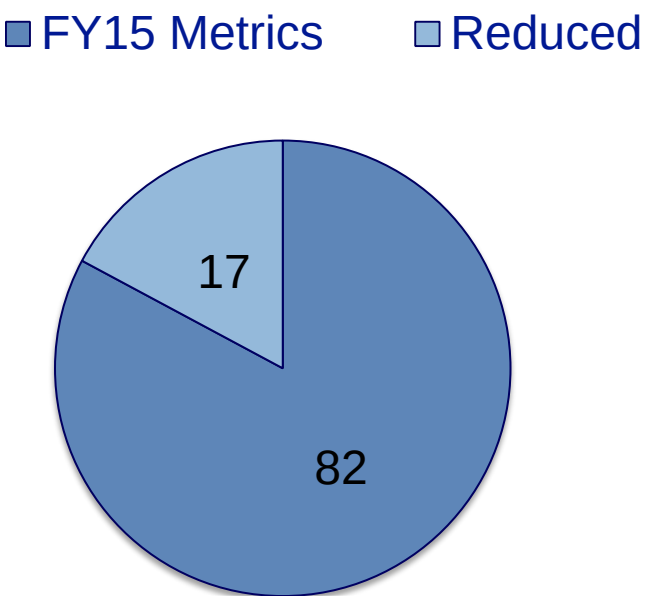
FY15 CIO FISMA Metrics Summary

- 82 Total Metrics
- *28 AP, 31 KFM, 23 BASE*
  - System Inventory: 11
  - ISCM: 21
  - ICAM: 14
  - Anti-Phishing and Malware Defense: 14
  - Data Protection: 8
  - Network Defense: 4
  - Boundary Protection: 4
  - Training and Education: 6
  - Incident Response: TBD

Homeland Security

FISMA Metrics Reduction

- Of the 97 metrics in the FY14 CIO Annual Metrics Release:
  - 56 were removed
  - 12 were reworded
  - 41 new metrics added
  - 29 substantially unchanged



Homeland Security

Residual Issues Presented by D/As to Address

- Definitions
  - Network Fabric; Privileged User; System; Common Configuration Baseline
- Source
  - Every metric not derived directly from a NIST 800-53 control (not required)
- Scope
  - FNR is adjudicating feedback and adding clarity to scope as necessary
- AP Metrics
  - Undergoing QC to make sure metrics are categorized appropriately

Homeland Security

FISMA Metrics

- Metrics are classified into three categories:
  - Administration Priorities (AP)
  - Key FISMA Metrics (KFM)
  - Baseline (BASE)

Homeland Security

New Cyber CAP Goals

- In accordance with The Government Performance and Results Modernization Act of 2010 EOP, has established these cyber priorities for FY15-17:
  - Information Security Continuous Monitoring—Provide ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity: posture, hygiene, and operational readiness.
  - Identity Credential and Access Management—Implement a set of capabilities that ensure users must authenticate to information technology resources and have access to only those resources that are required for their job function.
  - Anti-phishing and Malware Defense—Implement technologies, processes and training that reduce the risk of malware introduced through email and malicious or compromised web sites.
- There are 28 AP metrics in the FY15 CIO Metrics

Homeland Security

KFM Metrics

- KFMs are additional priority metrics outside of the CAP metrics that are scored.
- KFM are found in the following performance areas: system inventory, secure configuration management, vulnerability and weakness management, identity credential and access management, data protection, boundary protection, training and education, and incident response management.
- There are 26 KFM in the FY15 CIO Metrics

Homeland Security

Example: Software Asset Management

- 2.6. Percent (%) of endpoints from 2.1.2 covered by a desired-state software asset management capability to detect and block unauthorized software from executing (e.g. AppLocker, certificate, path, hash value, services, and behavior based whitelisting solutions). (AP)
- 2.7. How many major application databases does the organization maintain? (Base)
- 2.8. Percent (%) of the organization's network fabric that undergoes periodic discovery scanning specifically for the purpose of identifying and enumerating databases. (KFM)

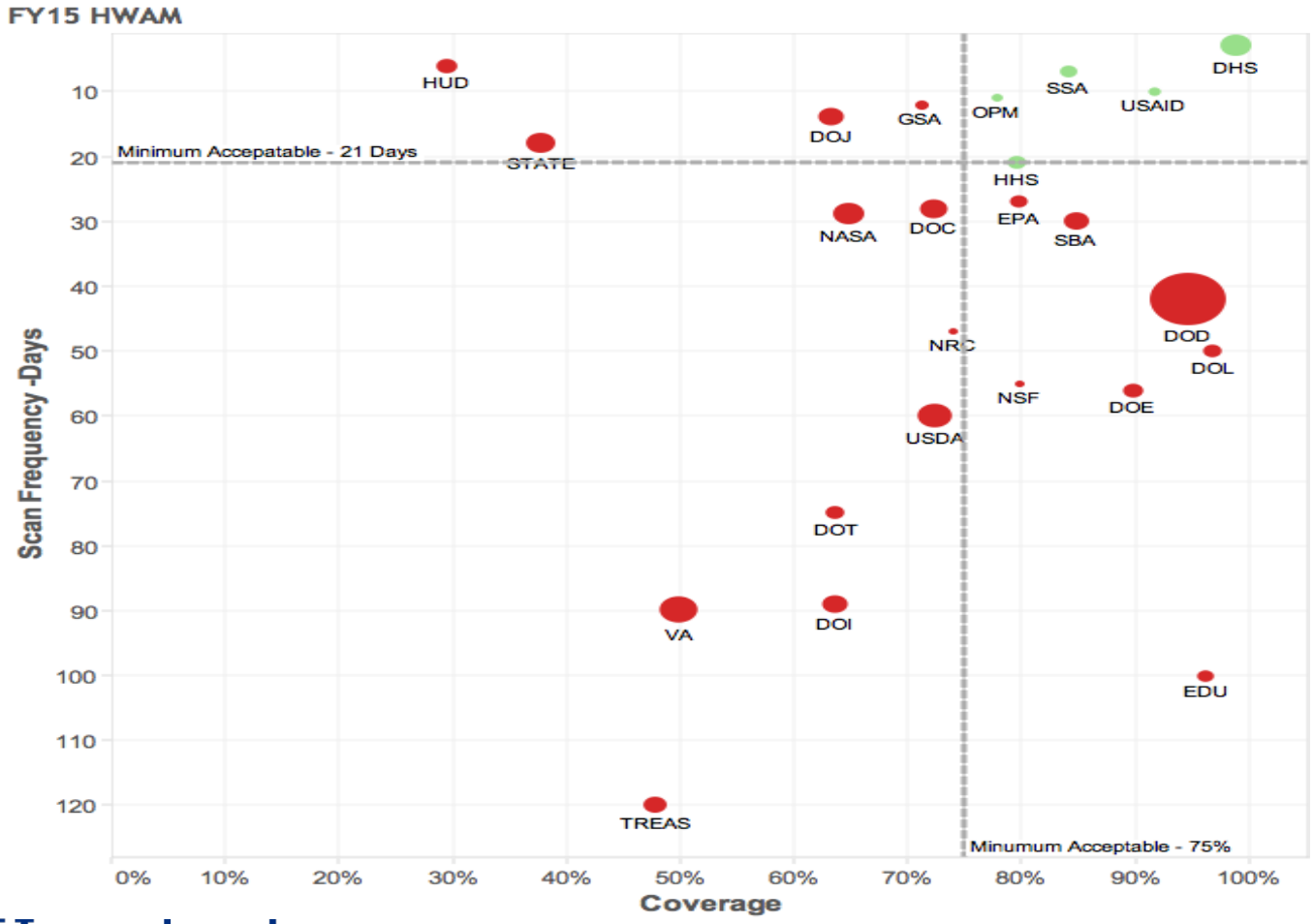
Homeland Security

Breaking It Down; AP

- 2.6. Percent (%) of endpoints from 2.1.2 covered by a desired-state software asset management capability to detect and block unauthorized software from executing (e.g. AppLocker, certificate, path, hash value, services, and behavior based whitelisting solutions). (AP)
- For AP metrics D/A are expected to:
  - Establish a plan-of-action for meeting the goal
  - Baseline current performance
  - Establish target performance that conforms to USG targets
  - Continuously monitor performance
  - Report results quarterly
  - Modify plan and targets as needed

Homeland Security

FY15 HWAM - where the interim goal is to cover ***n*** percent of the network with a scan every ***n*** days



Homeland Security

Breaking It Down: KFM

- 2.8. Percent (%) of the organization's network fabric that undergoes periodic discovery scanning specifically for the purpose of identifying and enumerating databases. (KFM)
- For KFM:
  - D/A head is responsible for determining the acceptable level of risk, with input from system owners, program officials, and CIOs
  - Utilize KFM as key indicators in determining an adequate level of security
  - Baseline current KFM performance
  - Establish target performance that conforms to D/A targets
  - Continuously monitor performance
  - Modify plan and targets as needed

FAQ: *How are KFM scored?*

- Because KFM are based on internal organization targets DHS does not calculate pass/fail scores for KFM.
- **However**, many KFM may be related to mandates that indicate 100% compliance.
- Reported results for KFM will be depicted alongside other D/A to show relative performance.
- A cumulative score for all KFM may be calculated.

D/A	27	28
Agency23	7739	100%
Agency3	9235	90%
Agency21	8285	90%
Agency5	1462	86%
Agency10	2839	78%
Agency20	313	72%
Agency13	9345	68%
Agency9	6036	66%
Agency16	2983	60%
Agency11	7658	50%
Agency4	8472	40%
Agency15	8236	40%
Agency17	4876	38%
Agency6	893	35%
Agency2	6623	20%
Agency7	5125	20%
Agency12	520	20%
Agency1	5585	0%
Agency8	292	0%
Agency14	3697	0%
Agency18	1311	0%
Agency19	7238	0%
Agency22	7037	0%
Agency24	7087	0%

Homeland Security

Breaking It Down: BASE

- 2.7. How many major application databases does the organization maintain? (Base)
- BASE metrics:
  - are not scored but are frequently used as a denominator for a scored metric
  - are used to establish current baselines against which future performance may be measured

Guidance

- Metrics and Guidance are subject to continuous improvement
  - Over 600 resource hrs. to-date responding to community feedback regarding FY15 CIO metrics
  - Active working group with members of the IG community on development of FY15 IG metrics
  - FY15 metric development is significantly ahead of last years schedule
- 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
Senior Advisor, Federal Network Resilience
Department of Homeland Security
Desk: 703-235-4945
Email: david.otto@dhs.gov

Homeland Security