

Continuous Monitoring: Diagnostics & Mitigation (FEDRAMP edition)


john.streufert@hq.dhs.gov
October 12, 2012

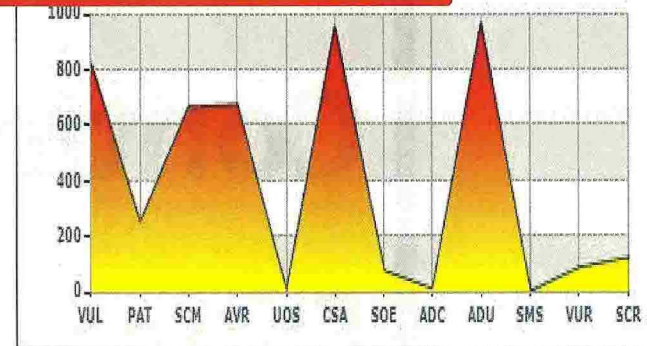


Homeland
Security

Organizations, Major Systems Contractor Performance

Risk Score Summary

Risk Level Grade	A+
Average Risk Score	5.0 
Site Risk Score	4,604.9
Scored Hosts	900
Rank in Enterprise	43 of 313
Rank in Region	10 of 42

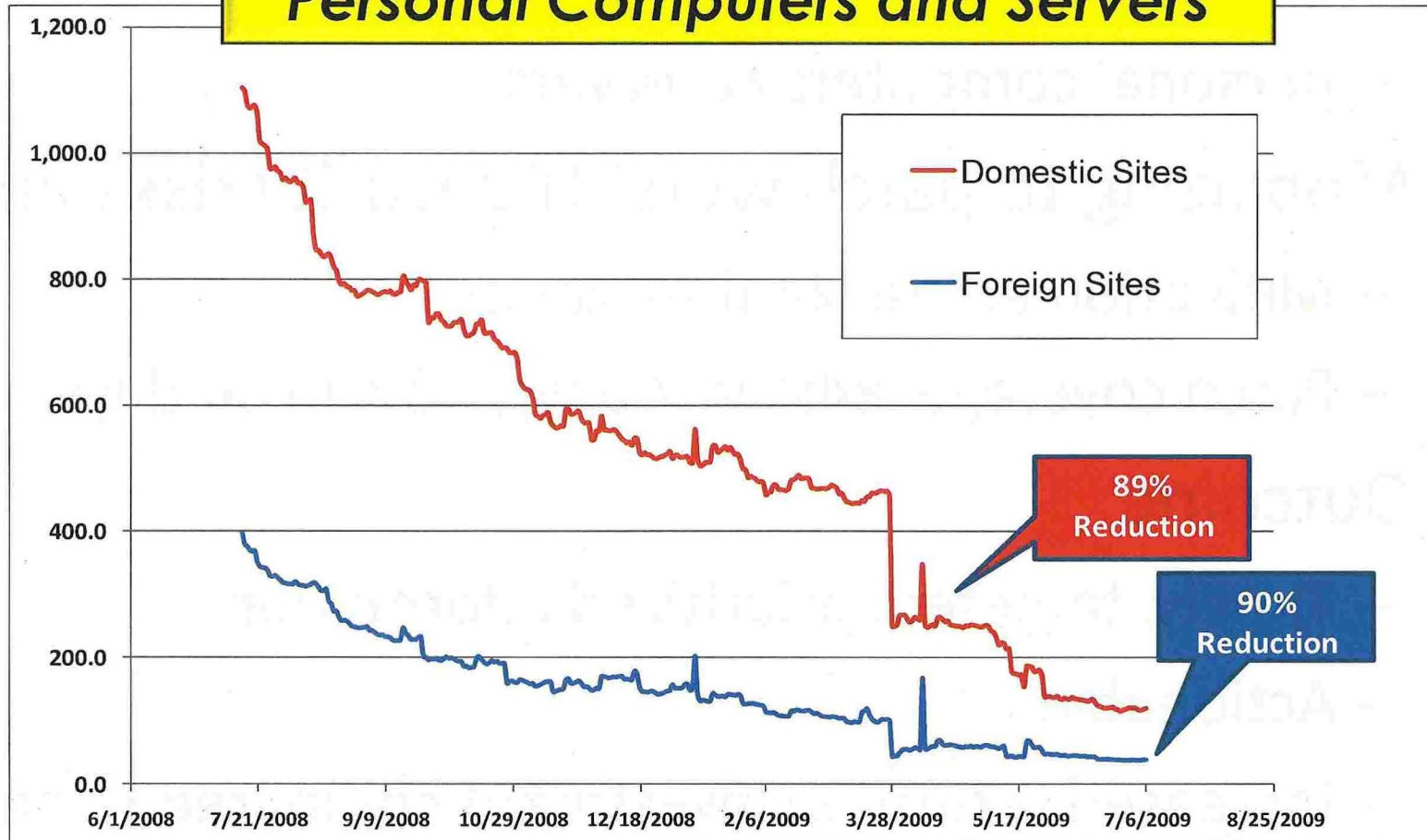


Component	Risk Score	Scored Objects	Avg/Object	% of Score	How Component is Typically Calculated
Vulnerability (VUL)	<u>821.9</u>	900	0.9	17.8%	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
Patch (PAT)	<u>250.0</u>	900	0.3	5.4%	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
Security Compliance (SCM)	<u>663.1</u>	900	0.7	14.4%	From .43 for each failed Group Membership check to .9 for each failed Application Log check
Anti-Virus (AVR)	<u>672.0</u>	900	0.7	14.6%	6 per day for each signature file older than 6 days
Unapproved OS (UOS)	<u>0.0</u>	900	0.0	0.0%	100 upon detection, then 100 per month up to a maximum of 500
CyberSecurity Awareness Training (CSA)	<u>948.0</u>	918	1.0	20.6%	After 15 days past the annual training expiration date, 1 per day up to a maximum of 90
SOE Compliance (SOE)	<u>75.0</u>	866	0.1	1.6%	5 for each missing or incorrect version of an SOE component
AD Computers (ADC)	<u>9.0</u>	900	0.0	0.2%	1 per day for each day the AD computer password age exceeds 35 days
AD Users (ADU)	<u>961.0</u>	1041	0.9	20.9%	1 per day for each account that does not require a smart-card and whose password age > 60, plus 5 additional if the password never expires
SMS Reporting (SMS)	<u>0.0</u>	900	0.0	0.0%	100 + 10 per day for each host not reporting completely to SMS
Vulnerability Reporting (VUR)	<u>85.0</u>	900	0.1	1.8%	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days
Totals:	4,604.9	--	5.0	--	



Results First 12 Months

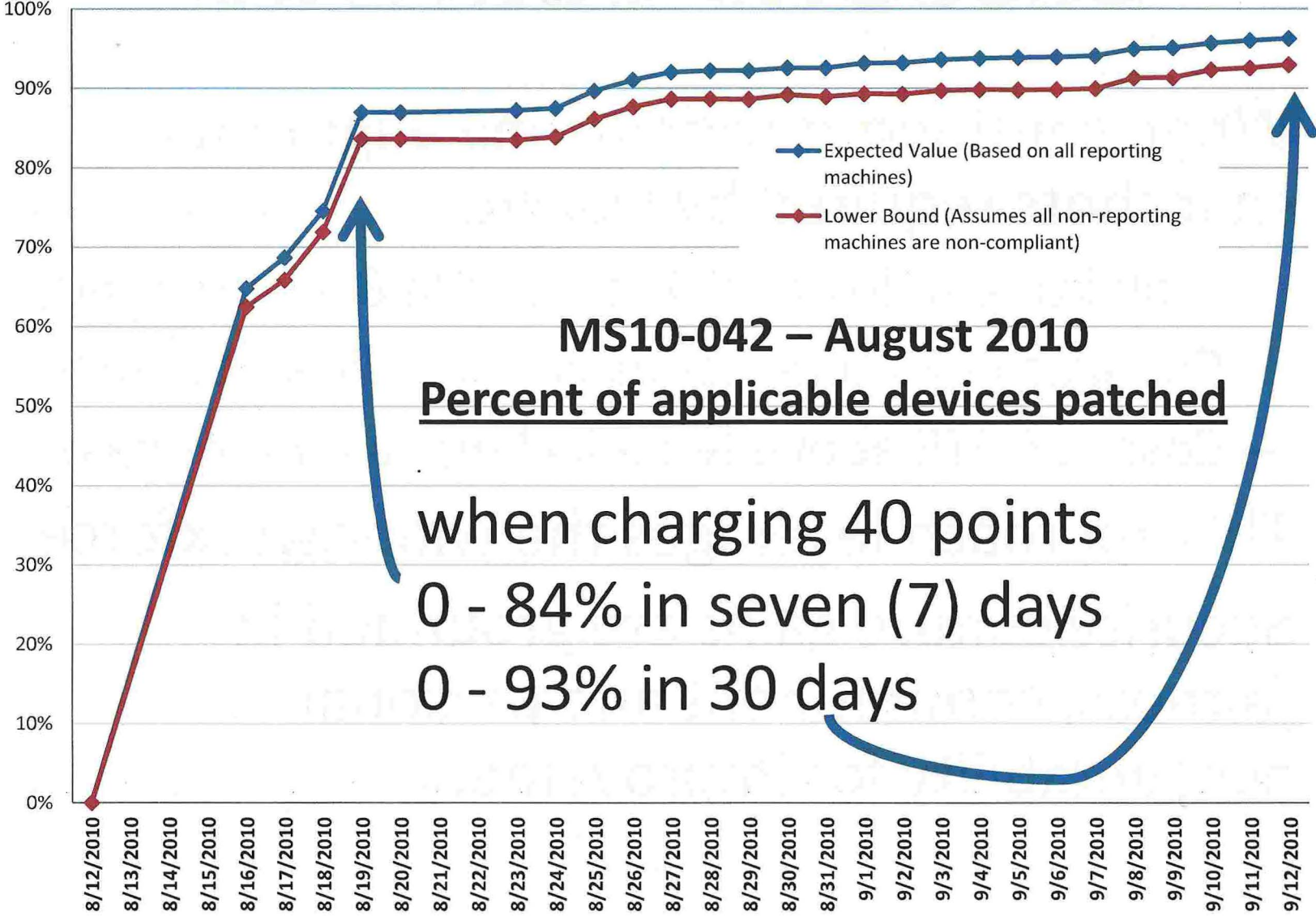
Personal Computers and Servers



Case Study Results

- 89% reduction in risk after 12 months
 - personal computers & servers
- Mobilizing to patch worst IT security risks first
 - Mitigation across 24 time zones
 - Patch coverage 84% in 7 days; 93% in 30 days
- Outcome:
 - Timely, targeted, prioritized information
 - Actionable
 - Increased return on investment compared to an earlier implementation of FISMA

Efficiency is Repeatable & Sustained



Lessons Learned

- When **continuous monitoring** augments snapshots required by FISMA:
 - Mobilizing to lower risk is feasible & fast (11 mo)
 - Changes in 24 time zones with no direct contact
 - Cost: 15 FTE above technical management base
- This approach leverages the wider workforce
- Security culture gains are grounded in fairness, commitment and personal accountability for improvement

Development Phase

Federal CIO and CISO Cyber Goals

- Protect information assets of the US gov't
 - Availability, integrity and confidentiality
- Lower operational risk and exploitation of
 - national security systems
 - .gov networks, major systems & **cloud services**
- Increase situational awareness of cyber status
- Improve ROI of federal cyber investments
- Fulfill FISMA mandates

Continuous Diagnosis and Mitigation (CDM)

“Full Operational Capability” (FOC) / Desired State:

- Minimum Time to FOC for CDM: 3 years;
- CDM Covers 80-100% of 800-53 controls;
- Smaller attack surface/“risk” for .gov systems;
- Weaknesses are found and fixed much faster;
- Replaces much 800-53 assessment work (\$440M)
 - And most of the POA&M process (\$1.05 B)
- Risk scores reflect: threat, vulnerability and impact
 - Used to make clear, informed risk-acceptance decisions
- Economies reduce total cost yet improve security.

Selection of First Year Priorities

- Implement CMWG focus areas for controls
 - NSA and CMWG collaboration put in pilots
 - Complete baseline survey of highest D/A risks
- Award task orders for sensors and services tailored to agency needs and risk profile
- Connect initial controls to dashboard
 - HW/SW asset management/white listing; vulnerability; configuration settings; anti-malware

Use of DHS Appropriated Funds

- Strategic Sourcing to buy
 - Sensors (where missing)
 - A Federal Dashboard
 - Services to operate the sensors and dashboard in the D/As
- Labor to mentor and train D/As to use the dashboard to reduce risk efficiently
- Processes to support CMWG (continuous C&A)

Stakeholder Consultation

- DHS and CMWG will consult on program direction and reflect stakeholder concerns of:
 - CIO Council/ISIMC, ISPAB
 - NSS, EOP, NIST, NSA
 - D/As and components
 - Industry
 - FFRDCs
 - Others

cdm.fns@hq.dhs.gov

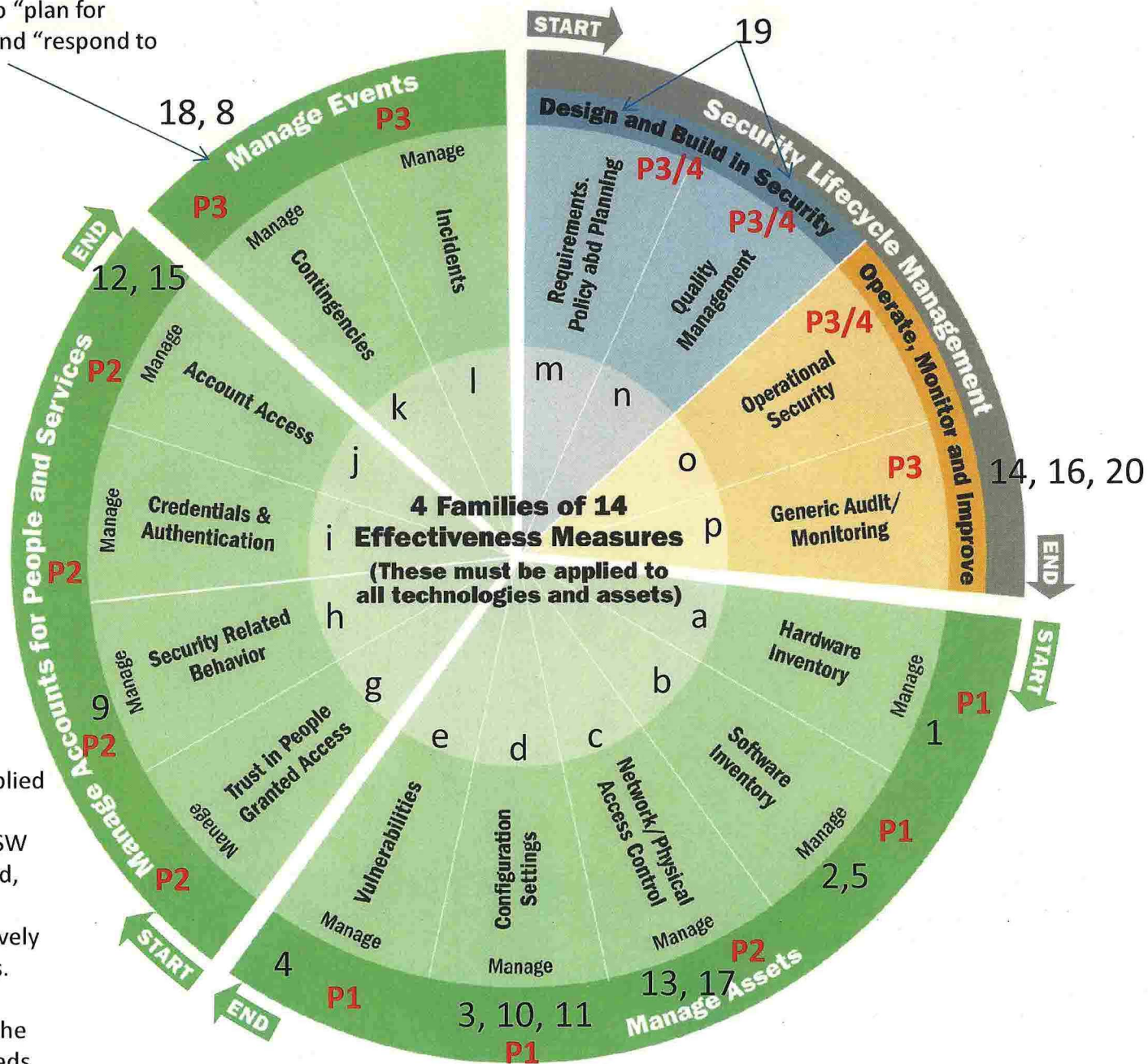
Cloud

Continuous Monitoring (CM) Contract Element	Beneficiary for FY13 Networks & COTS CM Software (\$202M)	Tools /Services as options for internal use	Use diagnostic standards but may or may not purchase
1. Dashboard	DHS pays for all government Department and Agencies Security reporting to Cyber Scope	<p>Can Purchase off of federal contract:</p> <ul style="list-style-type: none"> •.mil, Defense Industrial Base; • others who use federal \$; • plus State, local gov't 	Cloud Service providers for direct support of government dedicated cloud clients with cost embedded. CSP 's could buy dashboard.
2. Continuous Monitoring Tool Bundles (Multiple Award)	DHS Pays for initial .gov Agencies & Departments who choose diagnostic capabilities	<p>Can Purchase off of federal contract:</p> <ul style="list-style-type: none"> •.mil, Defense Industrial Base; • others who use federal \$; • plus State, local gov't 	Cloud Service Providers offer direct support of government dedicated cloud clients with cyber testing cost embedded. CSP 's could buy tools.
3. Continuous Monitoring as a Service (CMaaS)	DHS pays for initial .gov Agencies & Department who may choose a diagnostic service provider	<p>Department & Agencies (or others) pay for custom systems CM using internal C&A report money (diagnostics and feeds to Cyber Scope)</p>	Department & Agency custom systems using internal funds. CSP 's could buy CMaaS for use as 3 rd party Assessors.
4. Continuous monitoring data integration	DHS pays to prepare .gov diagnostic reports & CyberScope feeds	<p>Department & Agencies (or others) pay Using DHS published standards using internal funds</p>	Using DHS published standards using internal funds

\$440 M/yr

BACKGROUND

Change to "plan for events" and "respond to events".



6,7 are assets: They require all the other capabilities applied to them. For an application, it's HW, SW etc. must be managed, inside a boundary, configured and relatively free of vulnerabilities.

One delta would be the extra analysis SW needs pre-operations.