

Four Briefings

- A. Does history of continuous monitoring inform next steps (NIST 03/21/2011)
- B. FISMA 2.0 Project Origin (2009-2010)
- C. FISMA 2.0 Continuous Certification and Accreditation (late 2010, early 2011)
- D. FISMA 2.0 Enterprise Deployment (2010)

A. Does history of continuous monitoring inform next steps?



John Streufert (DOSCISO@state.gov)
Deputy Chief Information Officer for Information Security
US Department of State
March 21, 2011

Steps at the State Department

Continuous monitoring risk metrics – production 2009

Launch of iPost pilot for servers and PC's – July 2008

Agreement of 11 Ops Security organizations - 2007

IRM/IA & DS target scanning every 3 days–August 2006

CIO asks for leading IT Security program – Summer 2006

4 F's and 1 D minus in FISMA; Material Weakness

COTS Vulnerability & Config. Mang. Scanner – State 2005

Grades A-F Use Risk Points + Letters to Execs – USAID 2004

Increase Scanning to Every 3 Days – USAID late FY 2003

Gains in CMRS possible by:

- Correcting for “tunnel vision” seen in physiological studies of pilots**
- Using math and statistics to accelerate corrective action**
- Adapting market economics to risk**

[Automated patch distribution in combination with the above]

While not dramatically changing

- Structure of each Department
- Structure of major program delivery
- Decentralized management of technology decisions
- Cost by focusing on Return on Investment (ROI) of what was already being spent for defensive cyber security

OBSTACLE

CXOs are **accountable** for IT security

BUT

directly supervise only a small part of the systems actually in use.

RISK

Vulnerabilities - Now

The diagram illustrates the relationship between three stages of risk development. At the top is a green bar labeled 'Vulnerabilities - Now'. Below it is a yellow bar labeled 'Threat - In Development'. At the bottom is a red bar labeled 'Impact - In Development'. A thick black horizontal line runs across the middle, with two black arrows pointing upwards from it, one on the left and one on the right, indicating that vulnerabilities are being exposed or increased. Two blue arrows point downwards from the yellow bar, one on the left and one on the right, indicating that threats are being developed or increased. The bars are connected by a thick black horizontal line that runs across the middle of the diagram.

Threat - In Development

Impact - In Development

Threats Further Escalate

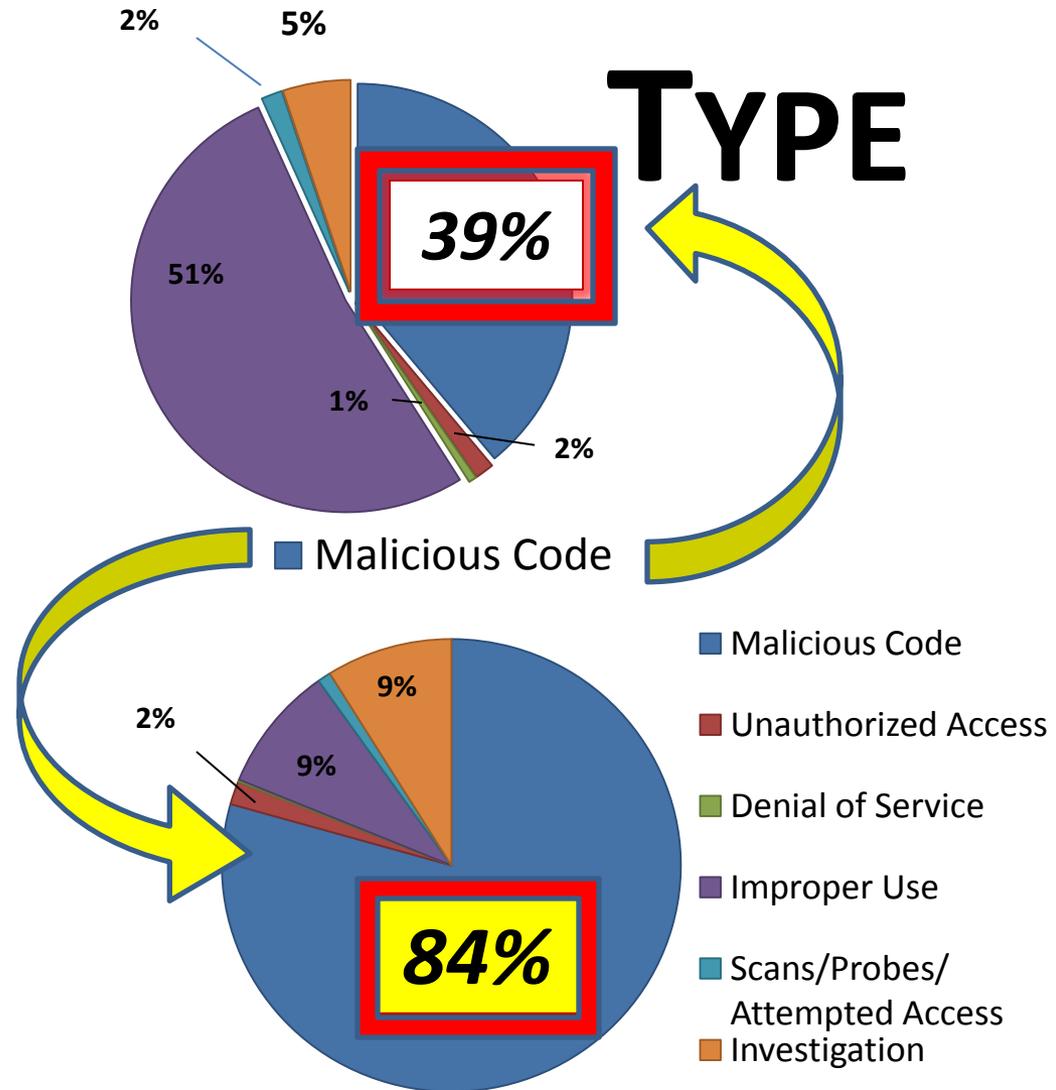
TICKETS

Year	Tickets
2008	2104
2009	3085
2010	7,998

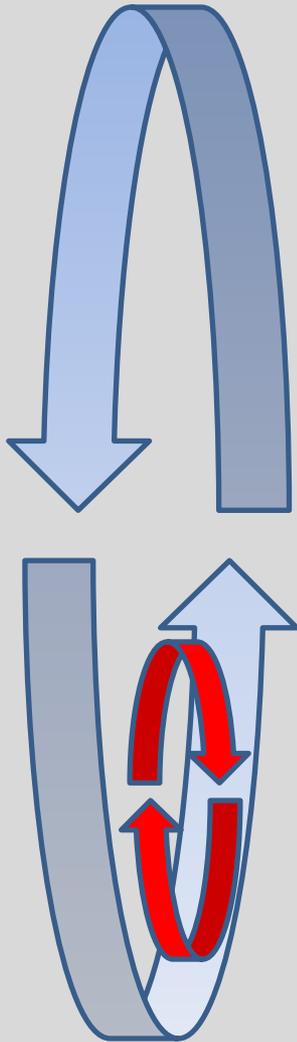
2008

2010

TYPE



Tactical Problem



- In combat whoever
“Observes – Orient¹ – Decides
– Acts” fastest wins.
- Cyber attacks are evolving
faster than they can be
counteracted outside DoD

¹ ‘OODA’ loops described in Boyd , The Fighter Pilot Who Changed the Art of War, by Robert Coram

Nature of Attacks

80% of attacks leverage
known vulnerabilities and
configuration management
setting weaknesses

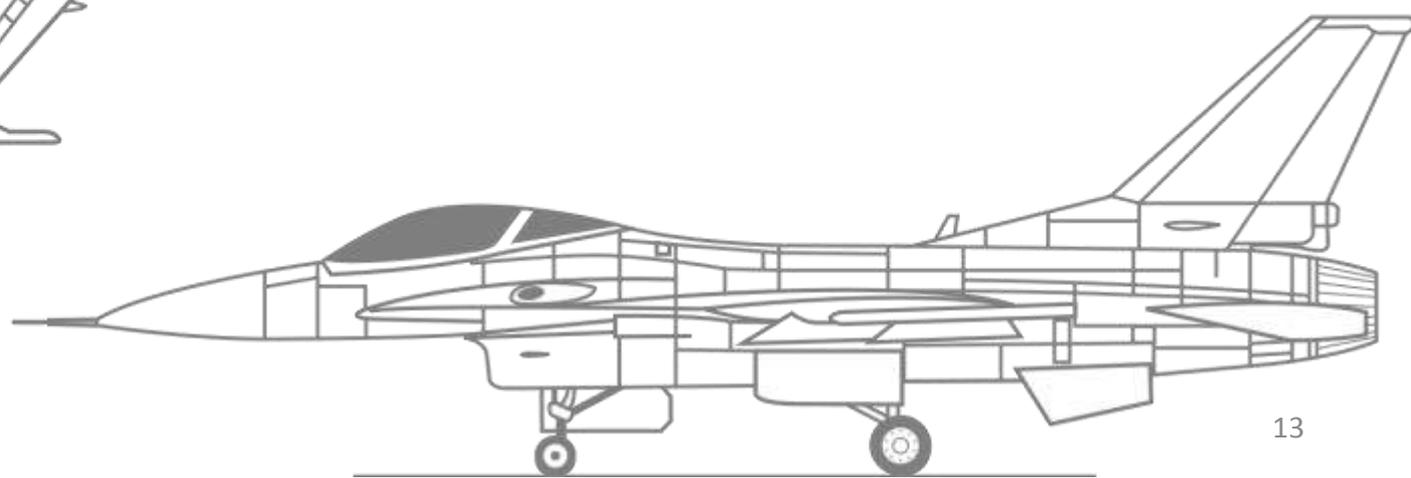
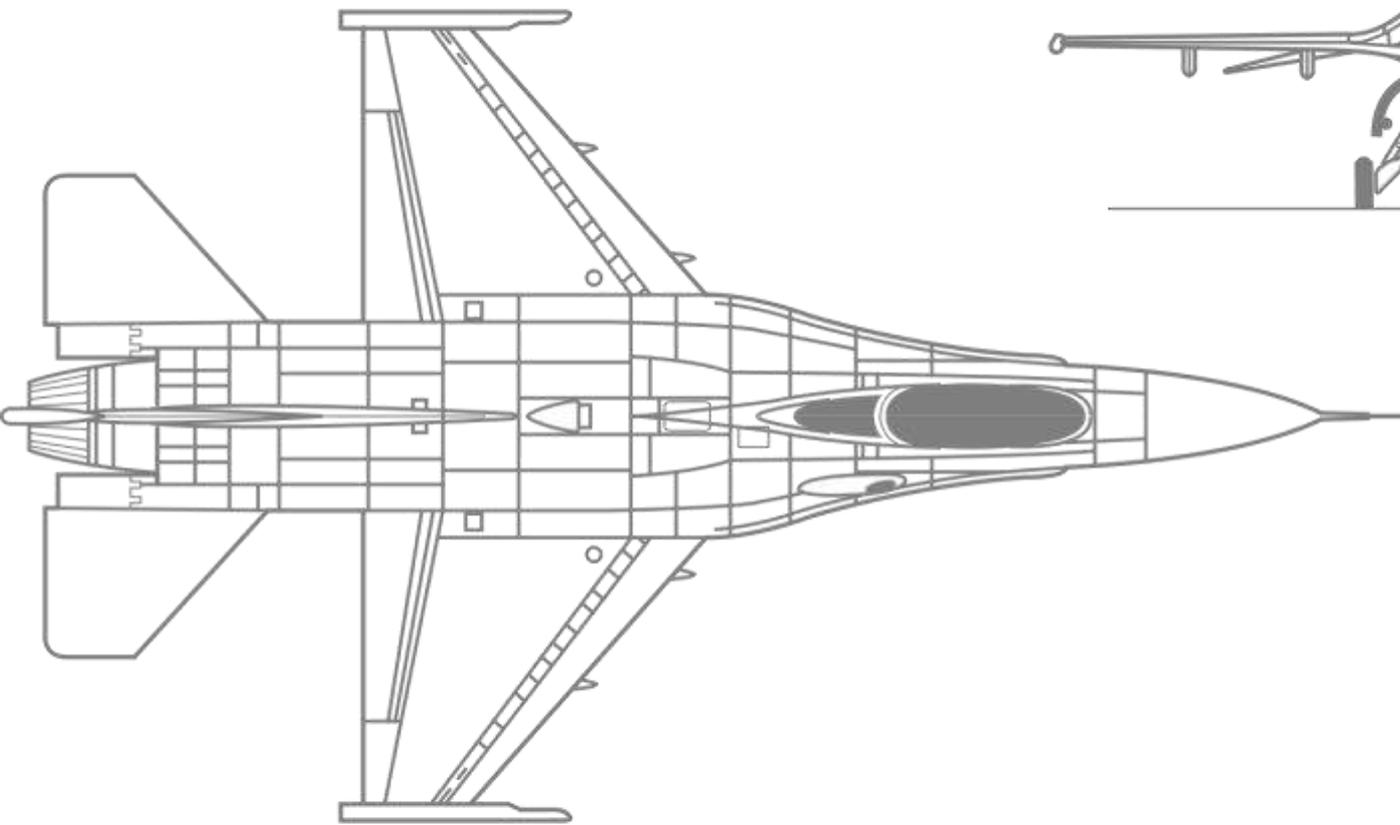
“Attack Readiness”

- What time is spent on
- Faster action =
lower potential risk

Objectives:



1. *Scan every 36-72 hours*
2. *Focus on Attack Readiness*
3. *Find & Fix Top Issues Daily*
4. *Personal results graded*
5. *Hold managers responsible*



Design ↔ Action



Addressing Information Overload

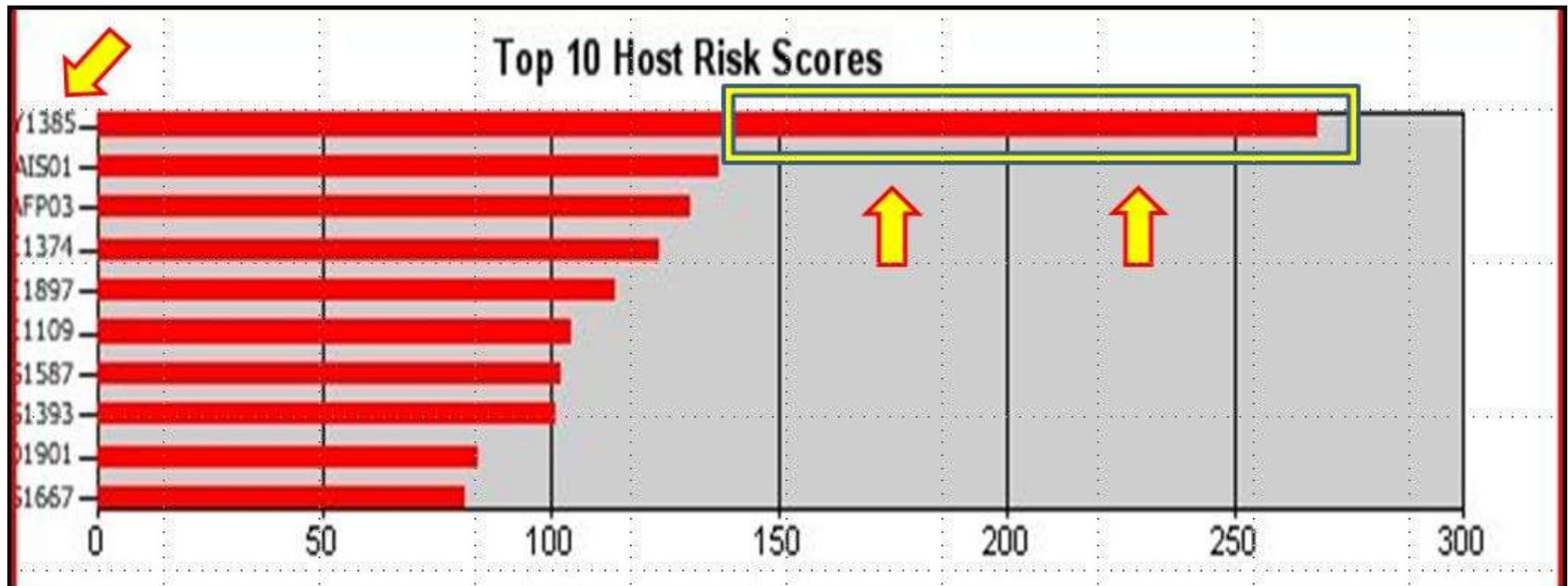
Component	Risk Score	Avg / Host	% of Score	How Component is Calculated
VUL - Vulnerability	947.0	3.0	10.9 %	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
PAT - Patch	603.0	1.9	6.9 %	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
SCM - Security Compliance	6,181.2	19.5	71.2 %	From .9 for each failed Application Log check to .43 for each failed Group Membership check
AVP - Anti Virus	0.0	0.0	0.0 %	6 per day for each signature file older than 6 days

Cube and Divide by 100

List Dominant Percentages of Risk

Graphics Guide Action

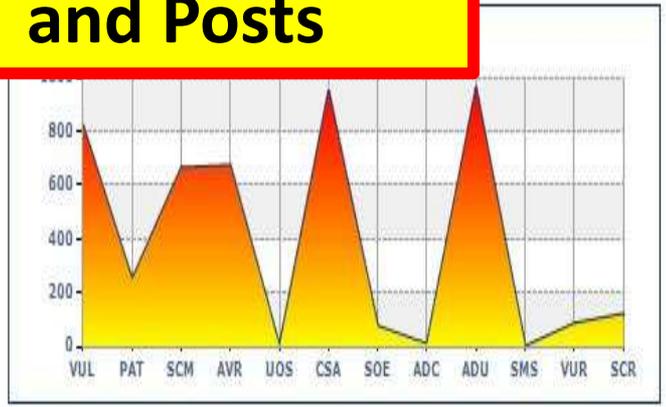
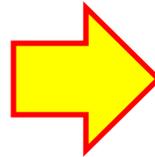
“Worst problems first”



Site Risk Scores for

Organizations and Posts

Risk Score Summary	
Risk Level Grade	A+ History
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

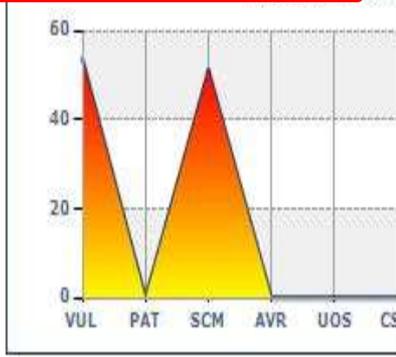


Component	Risk Score	Scored Objects	Avg/Object	% of Score	How Component is Typically Calculated
Vulnerability (VUL)	821.9	900	0.9	17.8%	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
Patch (PAT)	250.0	900	0.3	5.4%	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
Security Compliance (SCM)	663.1	900	0.7	14.4%	From .43 for each failed Group Membership check to .9 for each failed Application Log check
Anti-Virus (AVR)	672.0	900	0.7	14.6%	6 per day for each signature file older than 6 days
Unapproved OS (UOS)	0.0	900	0.0	0.0%	100 upon detection, then 100 per month up to a maximum of 500
CyberSecurity Awareness Training (CSA)	948.0	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)	75.0	866	0.1	1.6%	5 for each missing or incorrect version of an SOE component
AD Computers (ADC)	9.0	900	0.0	0.2%	1 per day for each day the AD computer password age exceeds 35 days
AD Users (ADU)	961.0	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)	0.0	900	0.0	0.0%	100 + 10 per day for each host not reporting completely to SMS
Vulnerability Reporting (VUR)	85.0	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	--	

Site Risk Scores for

Major Systems

Risk Score Summary	
Risk Level Grade	A+ History
Average Risk Score	8.1
Site Risk Score	104.9
Scored Hosts	13
Rank in Enterprise	79 of 313
Rank in Region	N/A



Component	Risk Score	Scored Objects	Avg/Object	% of Score	How Component is Typical
Vulnerability (VUL)	53.7	13	4.1	51.2%	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
Patch (PAT)	0.0	13	0.0	0.0%	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
Security Compliance (SCM)	51.2	13	3.9	48.8%	From .43 for each failed Group Membership check to .9 for each failed Application Log check
Anti-Virus (AVR)	0.0	13	0.0	0.0%	6 per day for each signature file older than 6 days
Unapproved OS (UOS)	0.0	13	0.0	0.0%	100 upon detection, then 100 per month up to a maximum of 500
CyberSecurity Awareness Training (CSA)	0.0	0	0.0	0.0%	After 15 days past the annual training expiration date, 1 per day up to a maximum of 90
SOE Compliance (SOE)	0.0	0	0.0	0.0%	5 for each missing or incorrect version of an SOE component
AD Computers (ADC)	0.0	13	0.0	0.0%	1 per day for each day the AD computer password age exceeds 35 days
AD Users (ADU)	0.0	0	0.0	0.0%	1 per day for each account that does not require a smart-card and whose password age > 60
SMS Reporting (SMS)	0.0	13	0.0	0.0%	100 + 10 per day for each host not reporting completely to SMS
Vulnerability Reporting (VUR)	0.0	13	0.0	0.0%	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days
Totals:	104.9	--	8.1	--	

Site Filter Options:

All Sites

SLA's

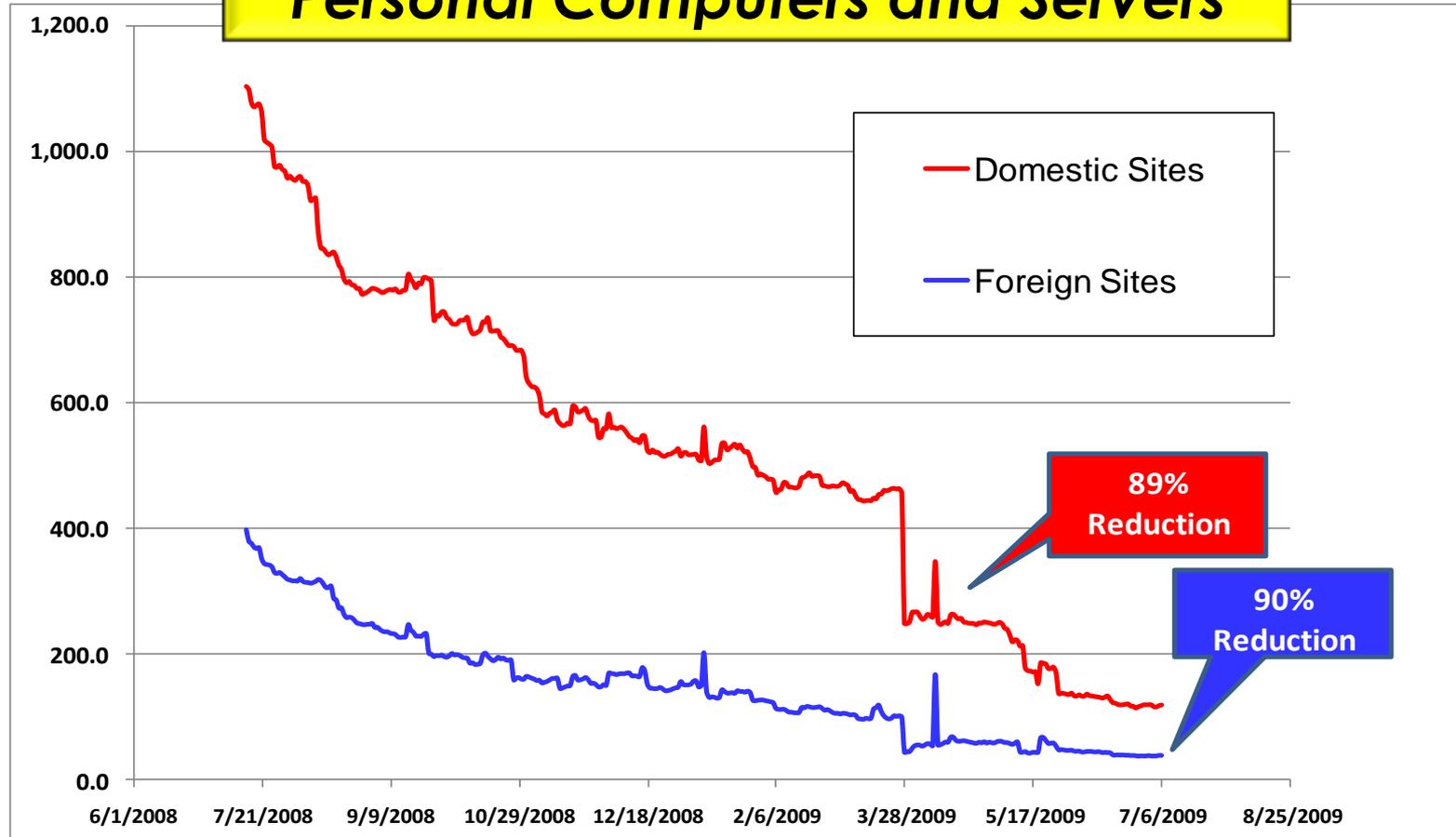
- Server Performance
- Network Latency
- Network Traffic
- Network Usage
- Performance Alerts
- Security**
- Compliance Scans
- Vulnerability Scans
- Active Directory
- CSA Training
- Patch Management
- Configuration**
- Processor
- Memory
- Logical Disk
- Operating System
- Software Products
- AntiVirus Status
- Services
- SMS Advertisements
- SMS Reporting





Results First 12 Months

Personal Computers and Servers



**Future Success
of FISMA 2.0
Guided By --**

#1: Our choices

CAG ID	Consensus Audit Guideline	NIST-800-53	US CERT Report
1	Inventory of authorized and unauthorized hardware	CM-1, CM-2, CM-3, CM-4, CM-5, CM-8, CM-9	[11 months before Feb 09] + 6 %
2	Inventory of authorized and unauthorized software	CM-1, CM-2, CM-3, CM-5, CM-7, CM-8, CM-9, SA-7	+ 22 %
5	Boundary Defense	AC-17, RA-5, SC-7, SI-4	+ 7 %
9	Controlled access based on need to know	AC-1, AC-2, AC-3, AC-6, AC-13	1 %
12	Anti-malware defenses	AC-3, AC-4, AC-6, AC-17, AC-19, AC-20, AT-2, AT-3, CM-5, MA-3, MA-4, MA-5, MP-2, MP-4, PE-3, PE-4, PL-4, PS-6, RA-5, SA-7, SA-12, SA-13, SC-3, SC-7, SC-11, SC-20, SC-21, SC-22, SC-23, SC-25, SC-26, SC-27, SC-29, SC-30, SC-31, SI-3, SI-8	+ 60%

#2: New Scoring Guidelines

9 factors beyond CVSS quantify
risk for action seeking
priorities among 20 Most
Critical & 800-53 controls

Component	Risk Score	Avg / Host	% of Score	How Component is Calculated
VUL - Vulnerability 	947.0	3.0	10.9 %	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
PAT - Patch	603.0	1.9	6.9 %	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
SCM - Security Compliance 	6,181.2	19.5	71.2 %	From .9 for each failed Application Log check to .43 for each failed Group Membership check
AVR - Anti-Virus	0.0	0.0	0.0 %	6 per day for each signature file older than 6 days
SOE - SOE Compliance	115.0	0.4	1.3 %	5 for each missing or incorrect version of an SOE component
ADC - AD Computers	26.0	0.1	0.3 %	1 per day for each day the AD computer password age exceeds 35 days
ADU - AD Users	222.0	0.7	2.6 %	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 - SMS Reporting	230.0	0.7	2.6 %	100 + 10 per day for each host not reporting completely to SMS
VUR - Vulnerability Reporting	84.0	0.3	1.0 %	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days
SCR - Security Compliance Reporting	279.0	0.9	3.2 %	After a host has no scans for 30 consecutive days, 5 + 1 per 15 additional days
Total Risk Score	8,687.1 	27.4 	100.0 % 	

For additional information on Risk Scoring, assistance with remediations, or to report suspected false positives, contact the IT Service Center to open a "Risk Score" ticket.

#3: Strategies for Enterprise Management

- **Risk Valuation**

Bad Things By The Numbers

Littering



Chemical Dumping

-- L.A. Hotel Fined --

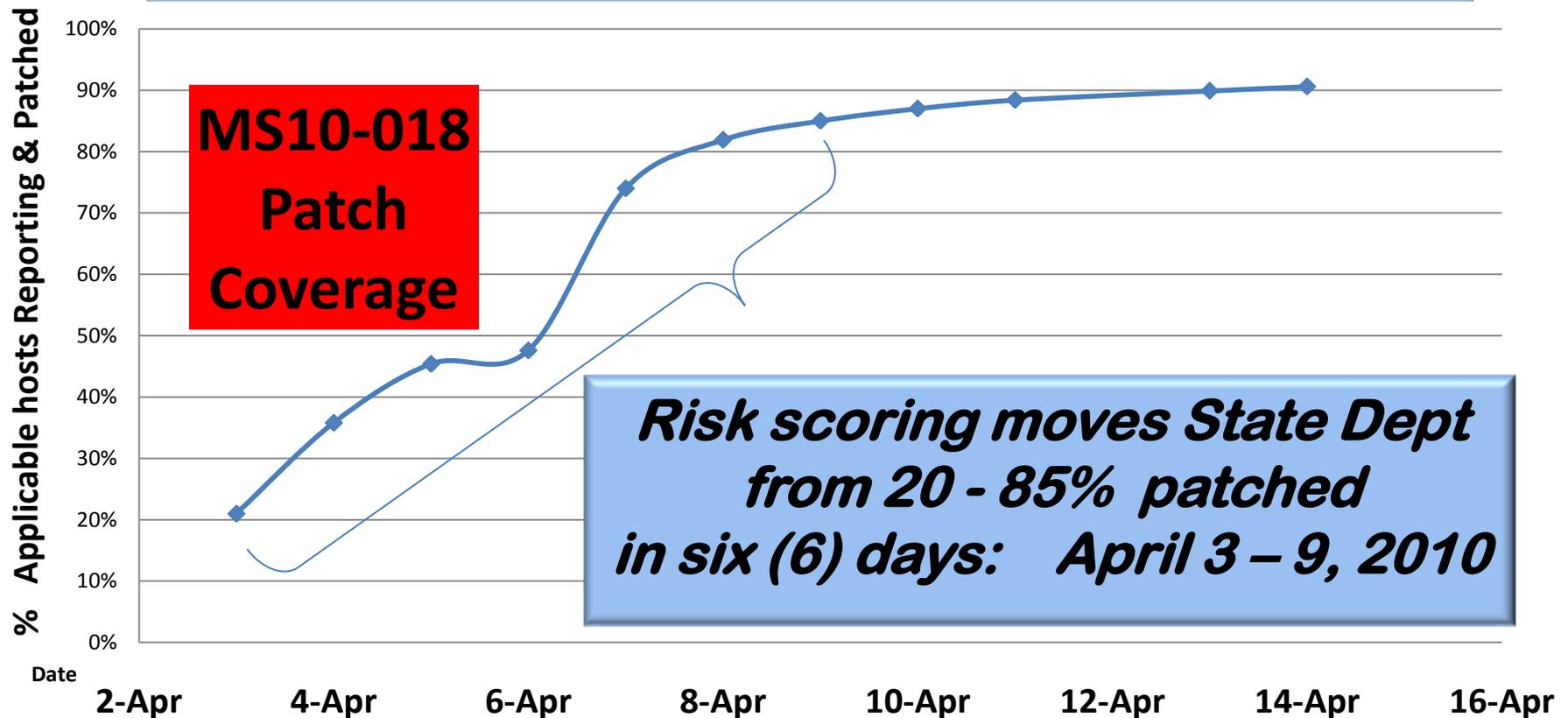
Hotel pays a
\$200,000 fine

because an employee dumps
pool chemicals into a drain
fumes fill a subway station
-- several people become ill

March 23, 2010

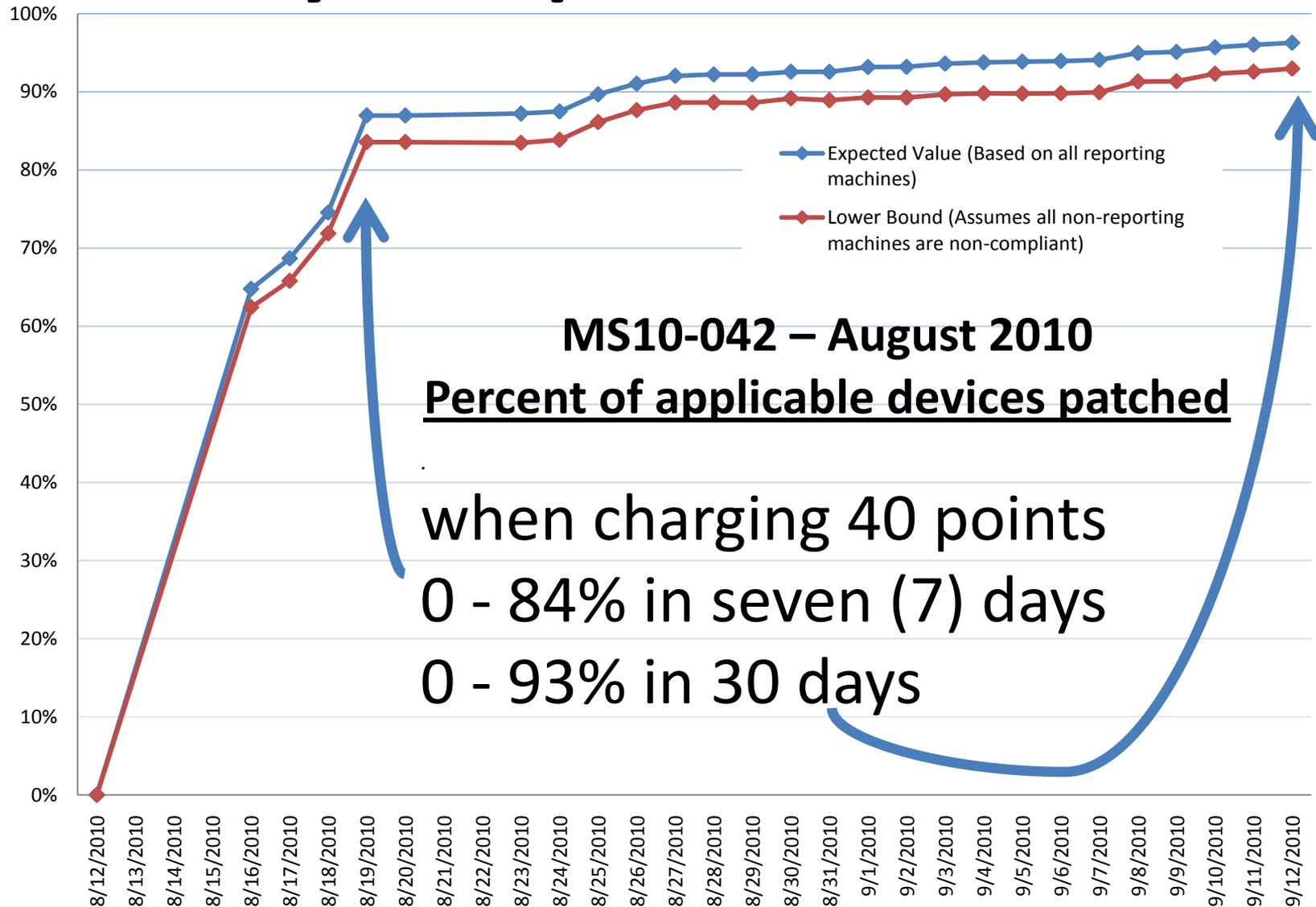
Call a Problem 40x Worse

Operation Aurora Attack



Risk valuation &
automated patching
distribution combined

Efficiency is Repeatable & Sustained



#4. Strategies for decentralized and fragmented delivery organizations

Risk Transfer Process

Vulnerability Exception Management

The following are the approved Risk Scoring exceptions for vulnerabilities

ID	Description	Affected Hosts	Owner	Implemented	Expires
#11002, SEP 11.x client <11.0.6200.754, A remote code execution vulnerability is present in some versions of Symantec Endpoint Protection. (Windows) (260)			IRM/SI/IIB - VIRT	Feb 24, 2011	Mar 24, 2011
11002	Symantec Endpoint Protection Manager Reporting Server Remote Code Execution Vulnerability	56,906			
WebPASS must be able to use JRE1.6.0_20 (127)			IRM/OPS/SIO	Jul 02, 2010	Mar 31, 2011
6620	Sun Java Runtime Environment LdapCtx Denial of Service Vulnerability	16,707			
6823	Sun Java Runtime Environment LDAP Serialization Code Execution Vulnerability	16,707			
6851	Oracle July 2009 Critical Patch Update	16,707			
6937	Sun Java Runtime Environment XML Digital Signature Authentication Bypass	16,707			
7059	Sun Java Runtime Environment Swing Denial of Service Vulnerability	16,707			
7060	Sun Java Runtime Environment JNLP File Denial of Service Vulnerability	16,707			
7062	Sun Java Runtime Environment Sensitive Information Disclosure Vulnerability (CVE-2009-2475)	16,707			
7063	Sun Java Runtime Environment Security Bypass Vulnerability (CVE-2009-2689)	16,707			
7064	Sun Java Runtime Environment Security Bypass Vulnerability (CVE-2009-2476)	16,707			
7065	Sun Java Runtime Environment Sensitive Information Disclosure Vulnerability (CVE-	16,707			

Transfer but Monitor

Taipei

Risk Scoring Exceptions

The following grading scale is provided by Information Assurance and may be revised periodically.

Site Risk Score	1,629.3
Average Risk Score	3.9
Risk Level Grade	A+
Total Site Exceptions	21,968.7
Average Without Exceptions	55.4

Average Risk Score		
At Least	Less Than	Grade
0.0	16.0	A+
16.0	35.0	A
35.0	65.0	B
65.0	95.0	C
95.0	115.0	D
115.0	150.0	F
150.0	-	F-

The following are the approved exceptions to Risk Scoring

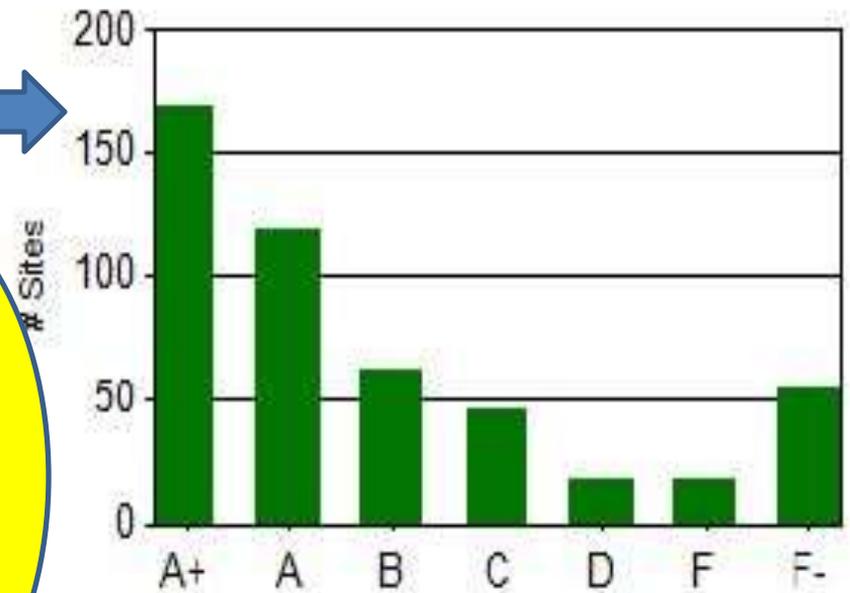
ID	Description	Implemented	Expires	Hosts	Owner	Score	Avg. Score
Vulnerability							
89	WebPASS must be able to use JRE1.6.0_20	Jul 02, 2010	Mar 31, 2011	139	RM/OPS/SIO	17,588.6	41.3

**If you
do this**

Status today

Average Risk Score		
At Least	Less Than	Grade
0.0	16.0	A+
16.0	35.0	A
35.0	65.0	B
65.0	95.0	C
95.0	115.0	D
115.0	150.0	F
150.0	-	F-

**16
points
per
device**



Risk Score Monitor Enterprise

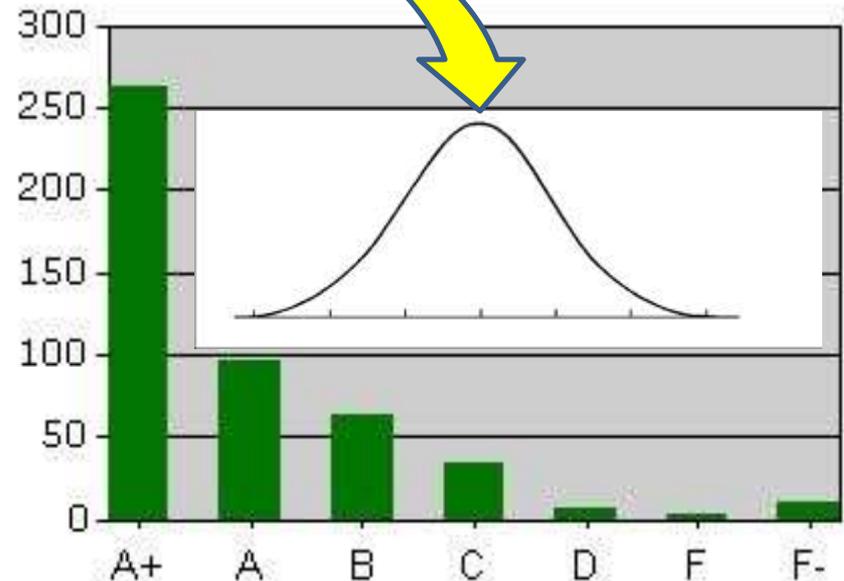
Total Hosts	32,366	51,157
Average Risk Score per Host	101.7	33.2

Grading Scale

Grade Dis

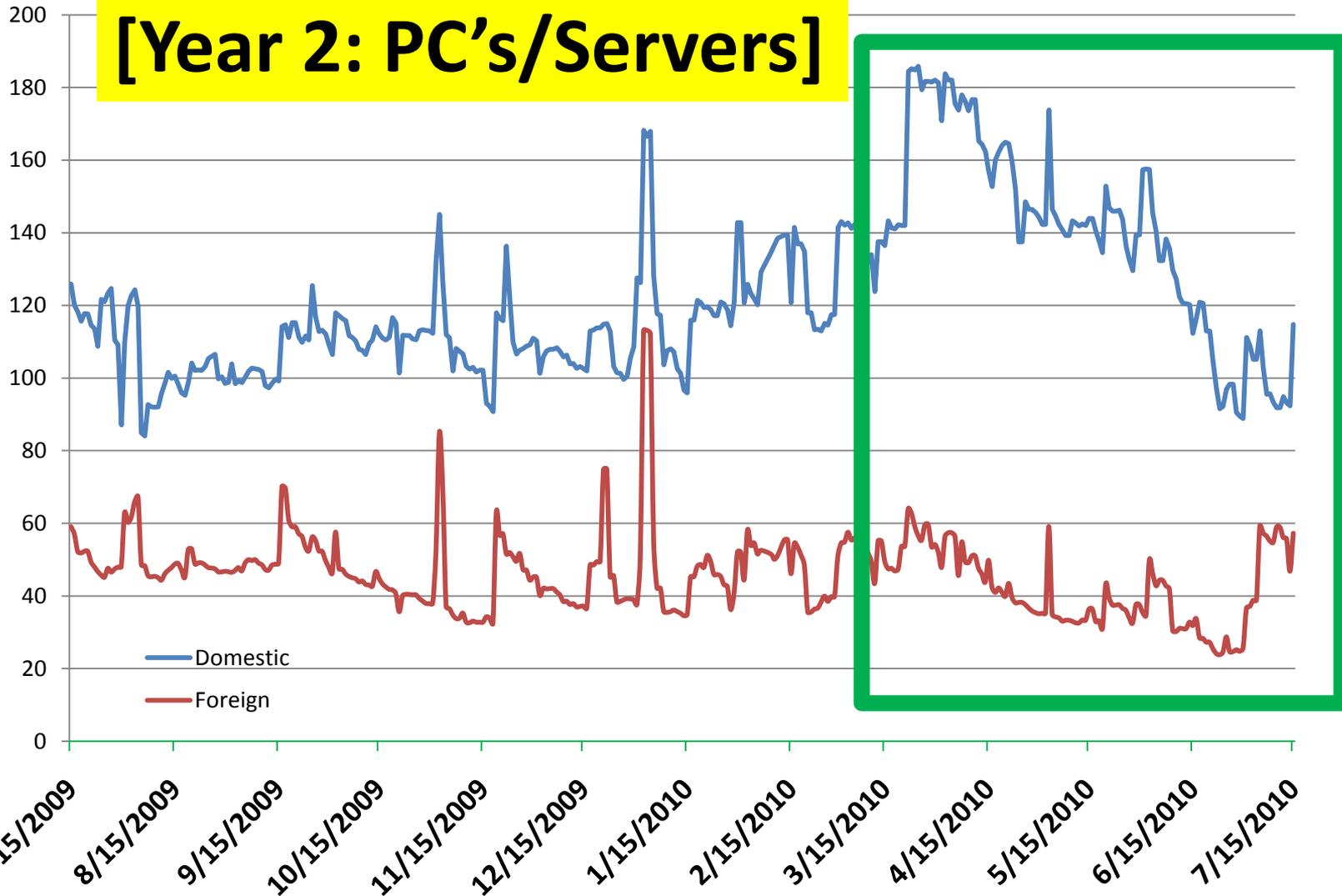
Average Risk Score			# Sites
At Least	Less Than	Grade	
0.0	40.0	A+	13
40.0	75.0	A	25
75.0	110.0	B	36
110.0	180.0	C	60
180.0	280.0	D	93
280.0	400.0	F	133
400.0	-	F-	

Sites

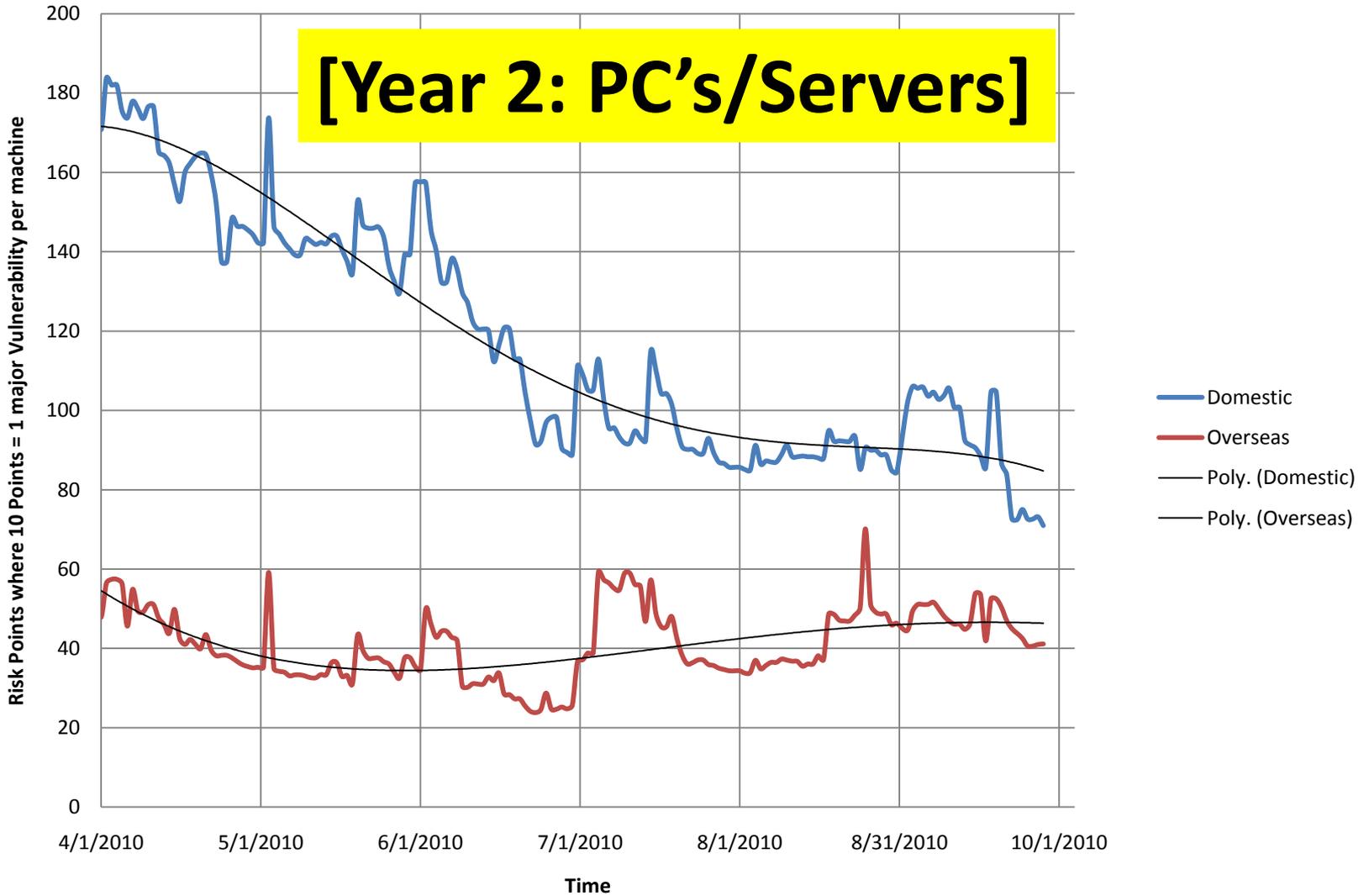


1/3 of Remaining Risk Removed

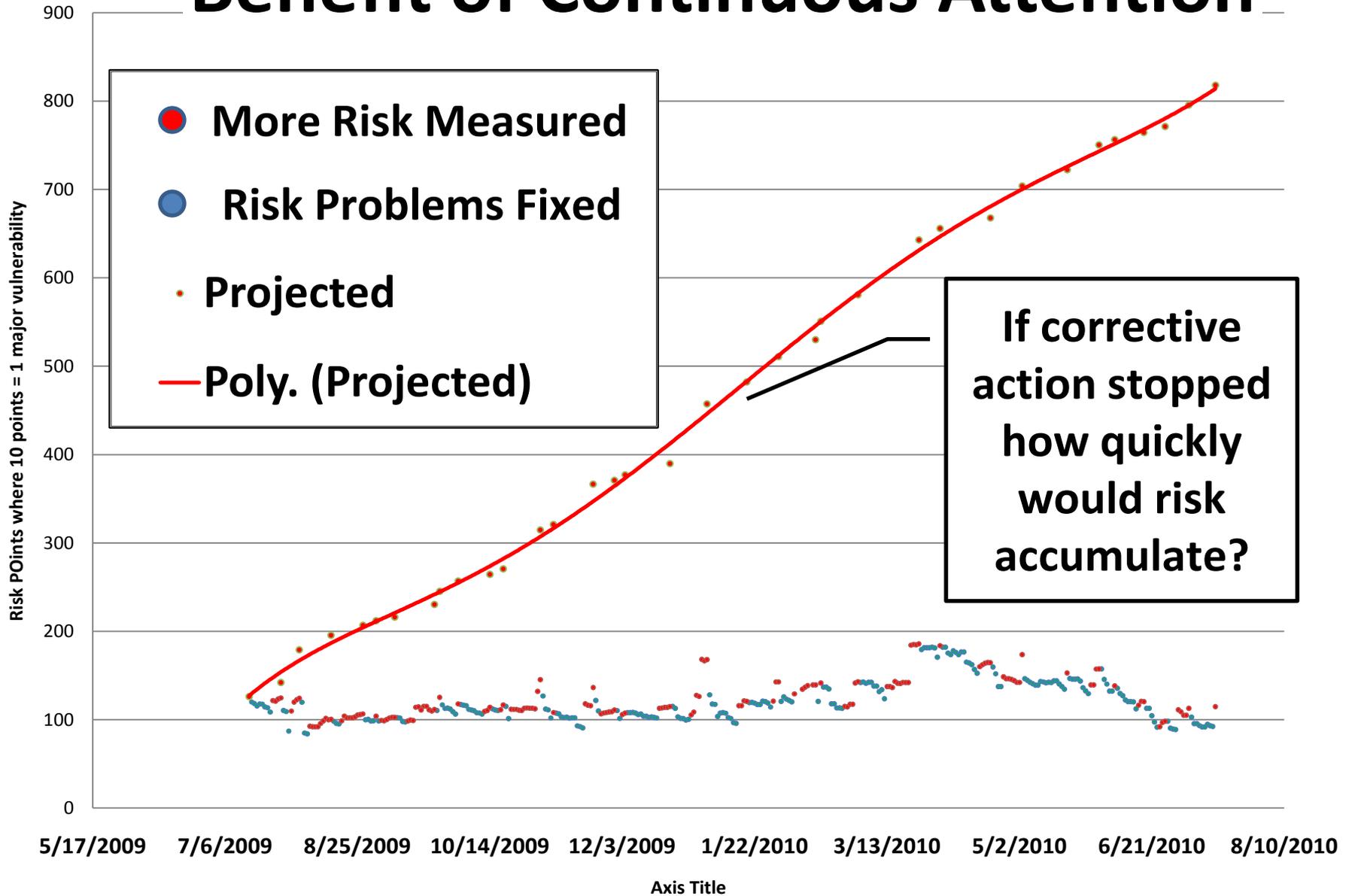
[Year 2: PC's/Servers]



Grade	Now	April	May	June	July	Aug	Sep
A+	40	36	31	27	22	18	13



Benefit of Continuous Attention



Tools support growth

Model Proposed:

- Multiple award contract from GSA/DHS/DoD
 - Dashboard, 15 tool groups, data integration
 - Separate contract for services
 - Scope Defense, DIB, federal, 50 states, local
- Industry will pursue SCAP improvements matching direction of a focused government strategy

Conclusions

- **Risk Scoring, Continuous Monitoring with Continuous Certification and Accreditation are scalable to large complex public and private sector organizations**
- **Higher ROI for continuous monitoring of technical controls as a substitute for paper reports**
- **Summarized risk estimates could be fed to enterprise level reporting**
- **Especially beneficial for decentralized programs**

B. FISMA 2.0

Project Origin



John Streufert (DOSCISO@state.gov)
Deputy Chief Information Officer for Information Security
US Department of State

FISMA 1.0

On December 17, 2002, the President signed into law the Electronic Government Act. Title III of that Act is FISMA, which *lays out the framework for annual IT security reviews, reporting, and remediation planning at federal agencies.* It requires that agency heads and IGs evaluate their agencies' computer security programs and report the results of those evaluations to OMB, Congress, and the GAO. ¹

¹ House Oversight and Government Reform website

OMB directs “*snapshots*” of process and compliance

1. “**Annual**” systems inventory
2. “**Annual**” testing
3. C&A[⌘] every “**three**” years
4. Weaknesses “**Quarterly**”
5. Train “**once a year**”
(awareness)

⌘ Certification and Accreditation studies

FISMA 2.0 Target

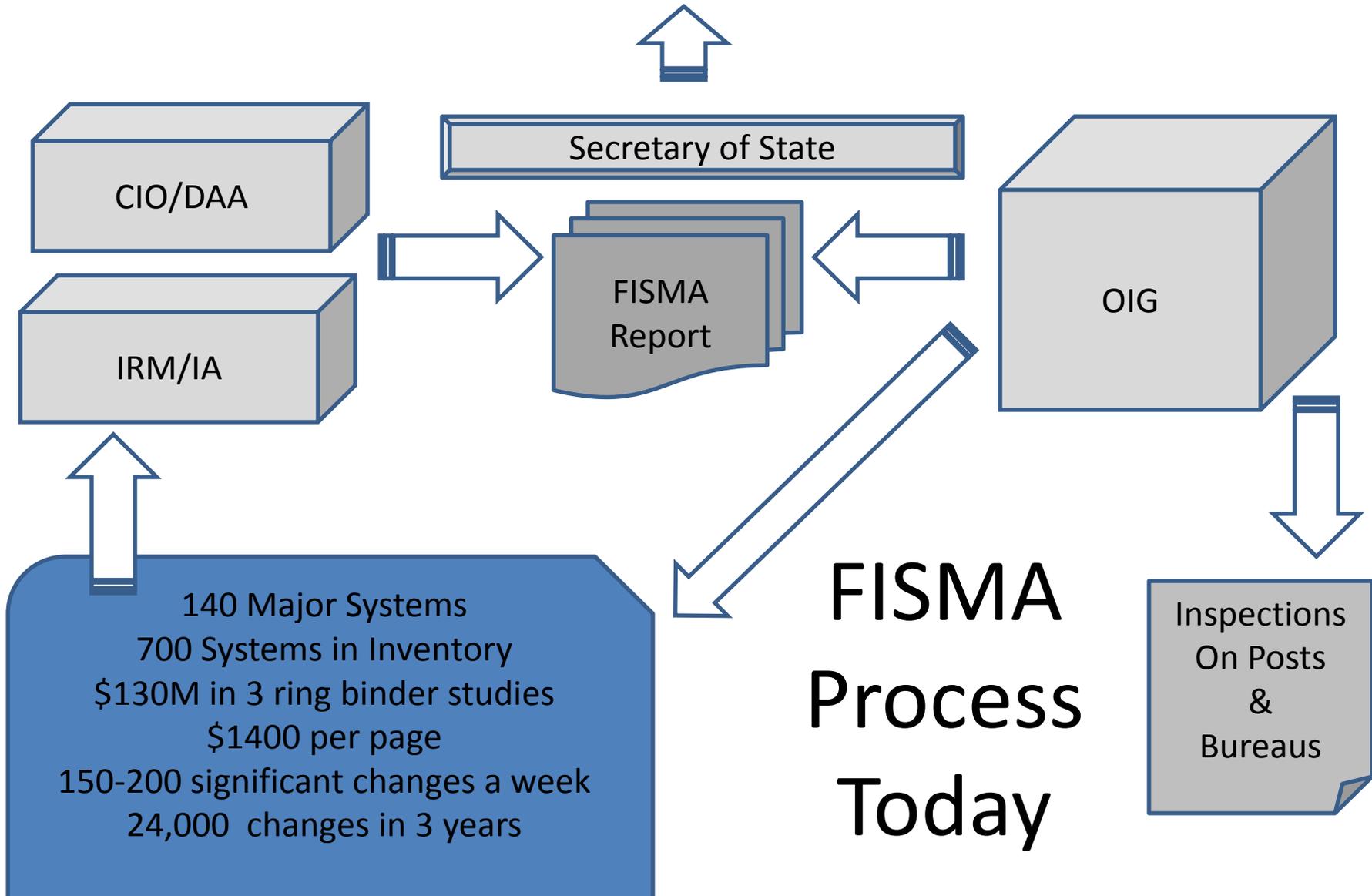
Continuous:

7. Incident Reporting
6. Configuration Management
5. “Daily” weakness updates
4. C&A technical controls **x 72** ✕
3. **Daily** not “**Annual**” testing
2. **Inventory** improvements
1. “**Daily**” awareness training

✕

Certification and Accreditation study of technical controls

Annual review to DHS, OMB & Congress



Why

and

How?

Focus on Gains

Technical control data efficiency:

- Every **2-15 days** not **3 years**

Create tiger teams for operations:

- inventory and to reduce site risks

C&A[ⓧ] cost down **56% then 62%**

- Invest in tool kits for everything
Support just in time for Certification & Accreditation[ⓧ]

Component	Risk Score	Avg / Host	% of Score	How Component is Calculated
VUL - Vulnerability 	947.0	3.0	10.9 %	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
PAT - Patch	603.0	1.9	6.9 %	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
SCM - Security Compliance 	6,181.2	19.5	71.2 %	From .9 for each failed Application Log check to .43 for each failed Group Membership check
AVR - Anti-Virus	0.0	0.0	0.0 %	6 per day for each signature file older than 6 days
SOE - SOE Compliance	115.0	0.4	1.3 %	5 for each missing or incorrect version of an SOE component
ADC - AD Computers	26.0	0.1	0.3 %	1 per day for each day the AD computer password age exceeds 35 days
ADU - AD Users	222.0	0.7	2.6 %	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 - SMS Reporting	230.0	0.7	2.6 %	100 + 10 per day for each host not reporting completely to SMS
VUR - Vulnerability Reporting	84.0	0.3	1.0 %	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days
SCR - Security Compliance Reporting	279.0	0.9	3.2 %	After a host has no scans for 30 consecutive days, 5 + 1 per 15 additional days
Total Risk Score	8,687.1 	27.4 	100.0 % 	

For additional information on Risk Scoring, assistance with remediations, or to report suspected false positives, contact the IT Service Center to open a "Risk Score" ticket.

Right Tools

Integrate Information & Tools

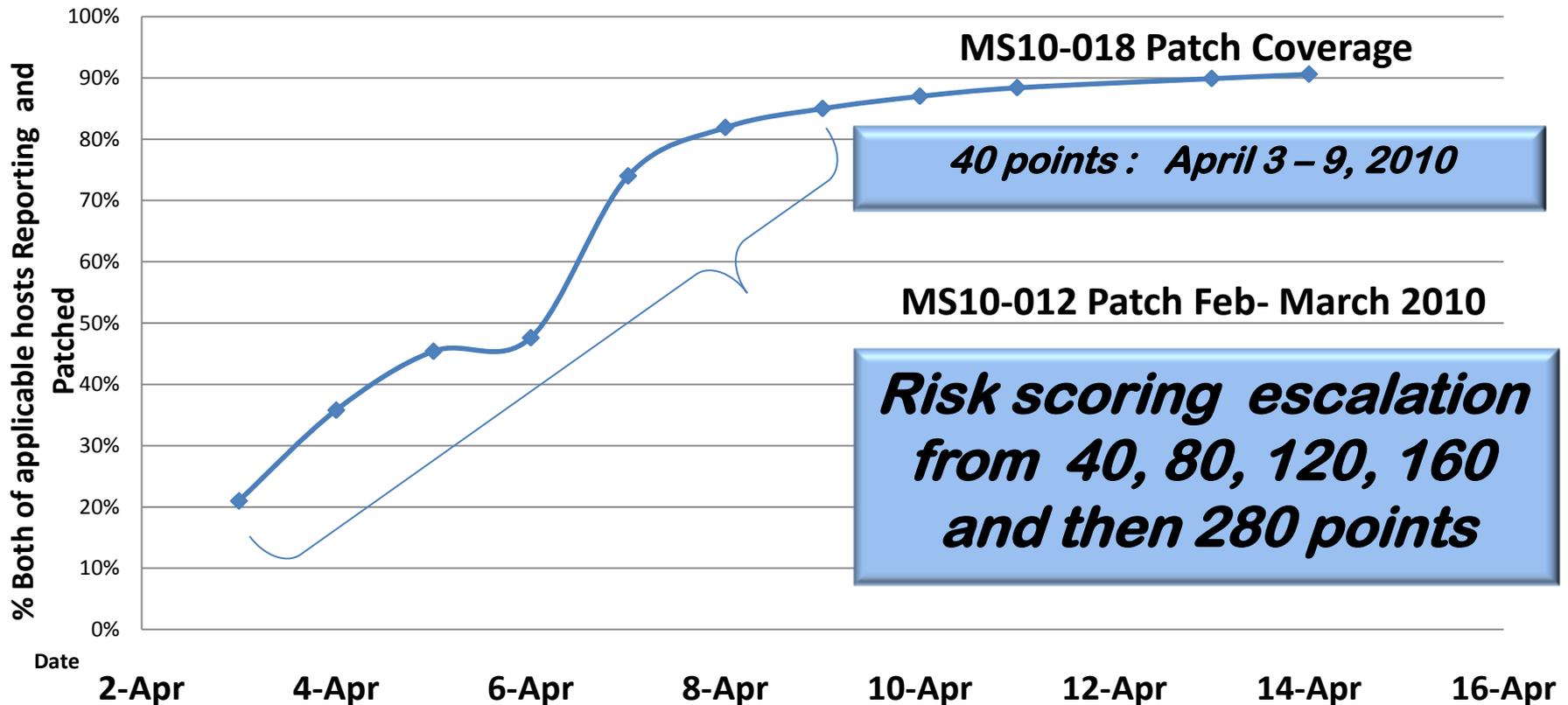
Timely – Targeted² – Prioritized

*“Metrics with
the Most Meaning”*

- ² The One to One Fieldbook: The Complete Toolkit for Implementing a 1 to 1 Marketing Program by [Don Peppers](#), [Martha Rogers](#), and [Bob Dorf](#)

Quantify Unique Threats

Google - Aurora Attack



**Embed Time &
Results Checks
into
Daily Operations**



Site Filter Options:

Foreign Domestic

Abidjan

Performance

Server Performance

Network Latency

Network Traffic

Network Usage

Performance Alerts

Security

Compliance Scans

Vulnerability Scans

Active Directory

Patch Management

Configuration

Processor

Memory

Logical Disk

Risk Scoring Reports

All Risk Scoring Exceptions

Enterprise Level

Enterprise and local risk scoring exceptions.

Vulnerability Management

Enterprise Level

Active scoring exceptions for vulnerabilities

Risk Score Rank

Site Level

Displays site risk score ranks in the enterprise

Enterprise Risk Score Monitor

Enterprise Level

Risk scores, grades, and rankings for each primary site in the Enterprise

Regional Risk Score Monitor

Regional Level

Risk scores, grades, and rankings for each site

Risk Scoring Exceptions

Site Level

Risk scoring exceptions applicable to the selected site

Site Collection Risk Score Monitor

Enterprise Level

Risk scores, grades, and rankings for each site in a named site collection

Risk Score Advisor

Site Level

Analysis assistance to facilitate improvement of risk score

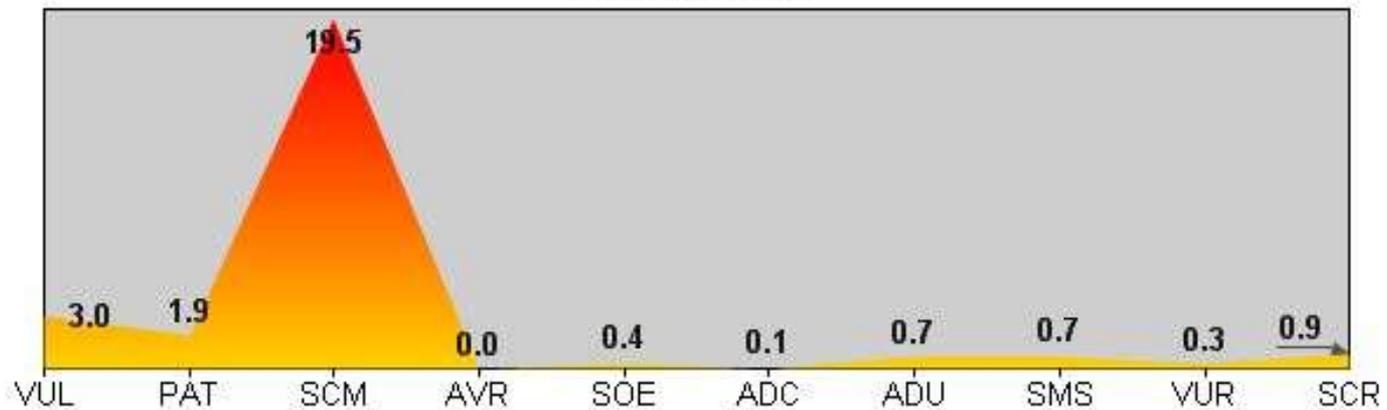
Risk Score Advisor

The following grading scale is provided by Information Assurance and may be revised periodically.

Site Risk Score	8,687.1
Hosts	317
Average Risk Score	27.4
Risk Level Grade	A+
Rank in Enterprise	163 of 438
Rank in Region	16 of 48

Average Risk Score		
At Least	Less Than	Grade
0.0	40.0	A+
40.0	75.0	A
75.0	110.0	B
110.0	180.0	C
180.0	280.0	D
280.0	400.0	F
400.0	-	F-

Risk Score Profile

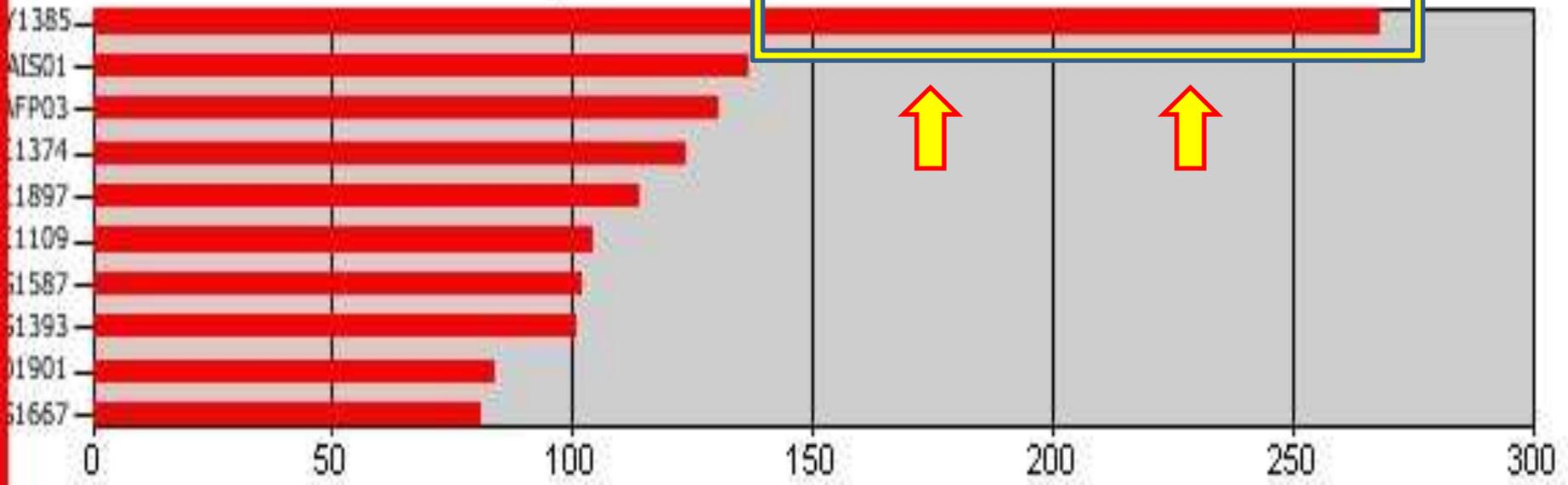


Component	Risk Score	Avg / Host	% of Score	How Component is Calculated
VUL - Vulnerability	947.0	3.0	10.9 %	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
PAT - Patch	603.0	1.9	6.9 %	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
SCM - Security Compliance	6,181.2	19.5	71.2 %	From .9 for each failed Application Log check to .43 for each failed Group Membership check
AVR - Anti-Virus	0.0	0.0	0.0 %	6 per day for each signature file older than 6 days
SOE - SOE Compliance	115.0	0.4	1.3 %	5 for each missing or incorrect version of an SOE component
ADC - AD Computers	26.0	0.1	0.3 %	1 per day for each day the AD computer password age exceeds 35 days
ADU - AD Users	222.0	0.7	2.6 %	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 - SMS Reporting	230.0	0.7	2.6 %	100 + 10 per day for each host not reporting completely to SMS
VUR - Vulnerability Reporting	84.0	0.3	1.0 %	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days
SCR - Security Compliance Reporting	279.0	0.9	3.2 %	After a host has no scans for 30 consecutive days, 5 + 1 per 15 additional days
Total Risk Score	8,687.1	27.4	100.0 %	

Cube and Divide by 100

For additional information on Risk Scoring, assistance with remediations, or to report suspected false positives, contact the IT Service Center to open a "Risk Score" ticket.

Top 10 Host Risk Scores



Risk Score History



Finding

**Details empower
technical managers**

*FOR TARGETED, DAILY
ATTENTION TO REMEDIATION*

**Summaries
empower executives**

*TO OVERSEE CORRECTION OF
MOST SERIOUS PROBLEMS*

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

Conclusions

- **Scalable to large complex public and private sector organizations**
- **Higher ROI for continuous monitoring of technical controls as a substitute for paper reports**
- Summarized risk estimates could be fed to enterprise level reporting

C. FISMA 2.0

Continuous

C&A



John Streufert (DOSCISO@state.gov)
Deputy Chief Information Officer for Information Security
US Department of State

**Shifting
earlier in
life cycle**

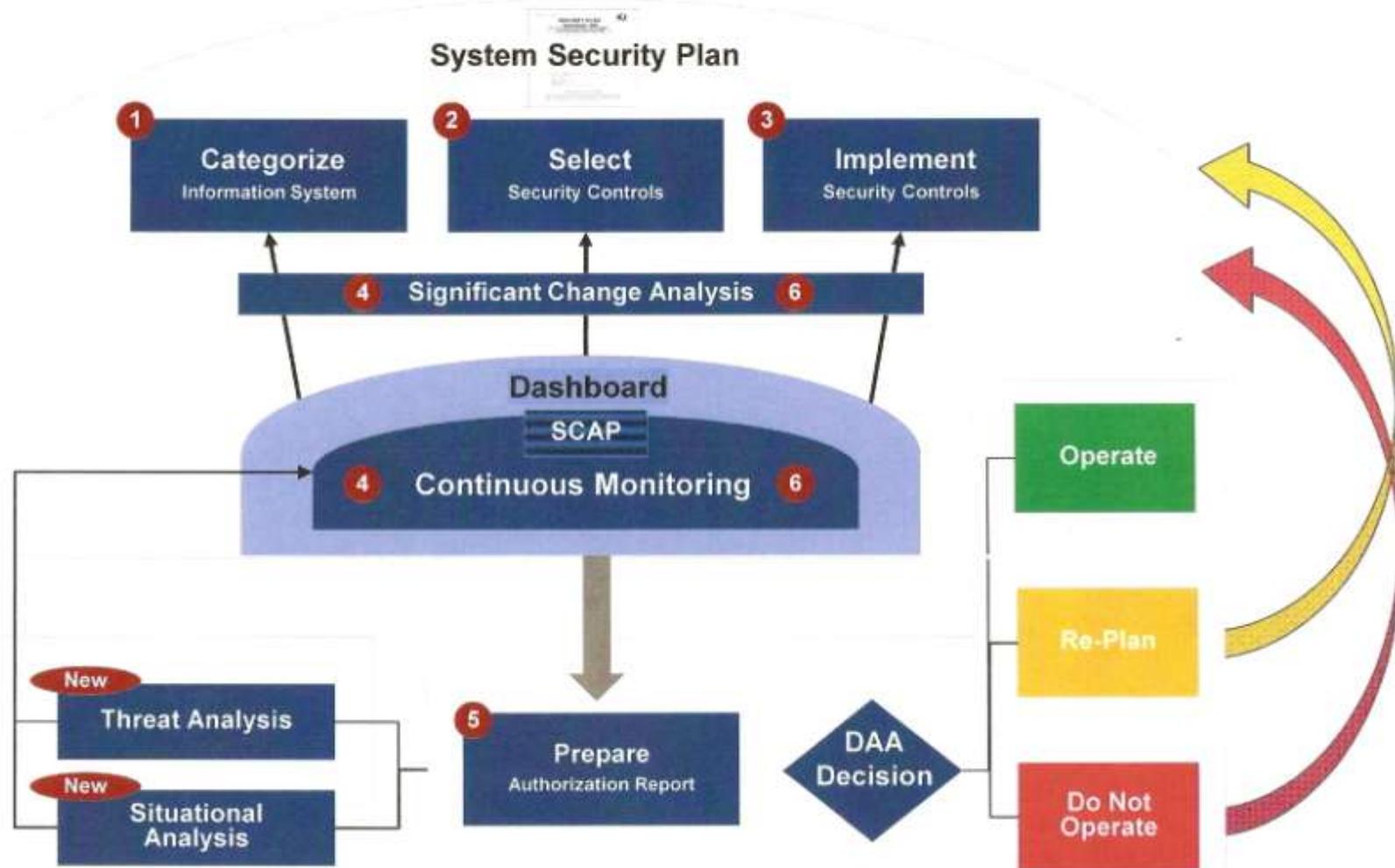
Should we position our best solutions before or after accidents?



Cofferdam unit departing Wild West in Port Fourchon on the Chouest 280 workshop named Joe Griffin 05 May 2010 -- Photo from BP.com

Continuous C&A Process will provide more effective real-time security – not just a snapshot in time

Continuous C&A Process



Focus on Gains

Technical control data efficiency:

- Every **2-15 days** not **3 years**

Create tiger teams for operations:

- inventory and to reduce site risks

⌘
C&A cost down 56% then 62%

- Invest in tool kits for everything
Support just in time for Certification & Accreditation ⌘

C&A Concerns

- a. Once in 3 year study of 110 technical, managerial and operational controls (NIST 800-53)
 - 25-2000 pages; \$30K - \$+2.5M
- b. Library cost: \$130M in 6 years
 - 95,000 pages @ \$1400 per page
- c. Changes: 150 - 200 a week;
 - 24,000 programs changed in 3 years

C&A Concerns

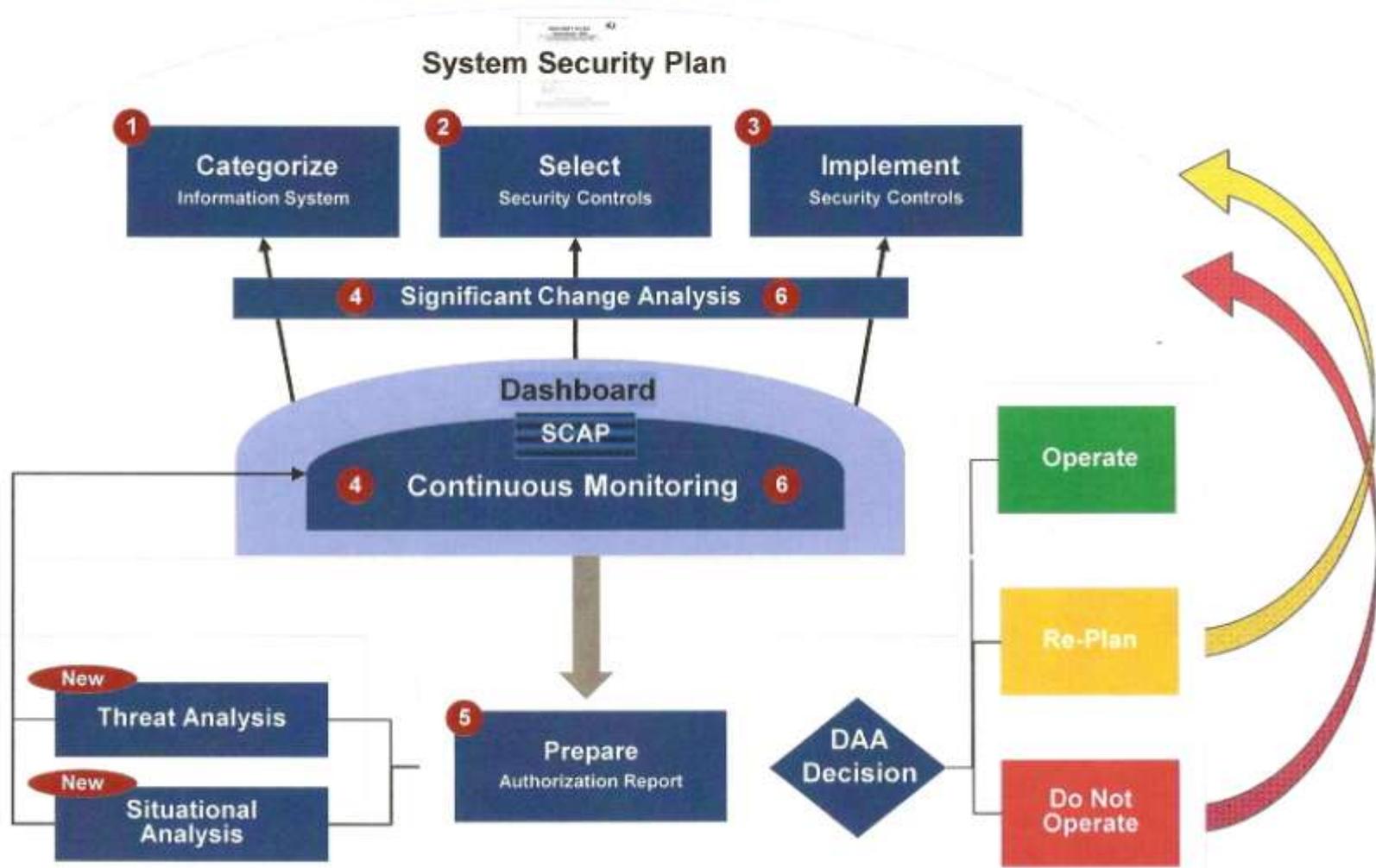
- d. Technical control sections are out of date rapidly
- e. C&A's focus on individual systems. Enterprise faces risk.
- f. Many attacks focus on subset of controls (CAG)

C&A

Improvement

Continuous C&A Process will provide more effective real-time security – not just a snapshot in time

Continuous C&A Process



Continuous C&A Pilots

Priority sequence: quick wins vs. long term:

- a. Inventory of Authorized Assets (CAG 1/2)
- b. Configuration and Vulnerability Monitoring
(CAG 3/4/10/12/13)
- c. SCAP Content (automated & non-automated testing)
- d. Boundary Defense (CAG 5/14)
- e. Situational Awareness and Threat Analysis
- f. Applications (CAG 7)
- g. Access Controls (CAG 6/8/9/11)
- h. Data Loss Protection (CAG 15)

Continuous C&A Pilots

A. Inventory of Authorized Assets (CAG 1-2)

Quick Wins	Long Term Strategy
<p>CAG 1: Use existing network tools (Campus Manager) to identify new devices to check against authorized inventory</p> <ul style="list-style-type: none">• Requires implementing these tools, network-wide.	<p>Refine the quick-win strategy. Maturing oversight processes. Implement Network-Access-Control (NAC, as feasible).</p>
<p>CAG 2: Use Windows Add-Remove Programs to identify software on Windows devices to check against authorized inventory.</p> <p>Use CCB and standard images for approved ARP entries.</p> <p>Map ARP to CPEs for FISMA reporting</p>	<p>Use authoritative white-listing tools for binary object level control. Maturing oversight processes.</p>

Continuous C&A Pilots

B. Configuration/Vulnerability Management

CAG 3-4-10-12-13

Quick Wins	Long Term Strategy
CAG 3/12: Continue current practices of scanning all Windows Devices.	Find more graceful way to manage transition between CM versions. Maturing oversight processes
CAG 4/10/13: Cover all network devices not covered by CAG 3 (Windows devices) using existing scanning tools.	Add scanning tools that may be needed beyond those currently available. Expand configuration standards to cover more device types. Use SCAP to define all configuration standards Maturing oversight processes

Continuous C&A Pilots

C. SCAP Content

Quick Wins	Long Term Strategy
Adopt and modify community SCAP content to cover as many needs as possible.	Find more graceful way to manage transition between CM versions. Maturing oversight processes.
Develop SCAP content and prototype tools to include covering: <ul style="list-style-type: none">• All test policy (including manual testing)• Configuration guides• SSP Control Lists• Test plans• Test specifications for sensors• Test Results• POA&M Tracking	Develop a community tool to efficiently write and display SCAP to support all functions listed on the left. Expand SCAP content to fully cover policy needs. Maturing oversight processes. Supports all CAG areas!!

Define once, use many!!

Continuous C&A Pilots

D. Boundary Defense (CAG 5/14)

Quick Wins	Long Term Strategy
<p>Get firewall rules under situational awareness tool oversight.</p> <p>Monitor for wireless access points, and remove from the network.</p>	<p>Model impact of changes to FW rules prior to changes and assess impact.</p> <p>Formally sunset all firewall rule exceptions, and require re-approval to continue.</p> <p>Implement internal segmentation of the network to reduce risks of threat by insiders and successful intruders.</p> <p>Maturing oversight processes.</p>

Continuous C&A Pilots

E. Situational Awareness and Threat Analysis

Quick Wins	Long Term Strategy
<p>Situational Awareness: Conduct pilots to identify attack paths using GOTS tools and find ways to block attacks on parts of the network.</p>	<p>Using lessons learned from quick wins, expand to the full network, using a COTS tool, if appropriate. Use capability to refine risk scoring and inform the DAA decision process. Maturing oversight processes.</p>
<p>Threat Analysis:</p> <ul style="list-style-type: none">• Continue current practices.• Use Existing Threat Analysis capability to refine risk scoring.• Use DHS penetration team on any system late for C&A.	<p>Find ways to refine these practices. Use to inform the DAA decision process. Maturing oversight processes.</p>

Continuous C&A Pilots

F. Applications (CAG 7)

Quick Wins	Long Term Strategy
<p>Expand use of existing monitoring to cover GSS support for each system.</p> <p>Pilot tools (in the areas specified by CAG) to identify utility of these tests.</p> <ul style="list-style-type: none">• Code Reviews (common weakness)• Web Application Scanning• DB Scanning• I/O Data Filtering <p>Establish OCIL checklists for critical points in the acquisition-development lifecycle</p>	<p>Place piloted tools into general production, at least by system integration test, and preferably sooner.</p> <p>Build security into the acquisition-development lifecycles.</p> <p>Training acquisition-staff/developers/owners in security management.</p> <p>Maturing oversight processes.</p>

Continuous C&A Pilots

G. Access Controls (6/8/9/11)

Quick Wins	Long Term Strategy
<p>Automated identification of accounts with elevated privileges and increase scoring of weaknesses on those account in proportion to the level of privileges.</p> <p>Make the full impact of access control lists transparent.</p> <p>Explore log data-mining tools.</p> <p>Identify rules to highlight significant events and eliminate “white noise”.</p>	<p>Reverse engineer roles that explain current access patterns based on user attributes.</p> <p>Find anomalies given those rules and investigate as suspicious.</p> <p>Identify refined rules to identify and highlight unusual access, eliminating “white noise”.</p> <p>Maturing oversight processes.</p>

D. FISMA 2.0

Enterprise

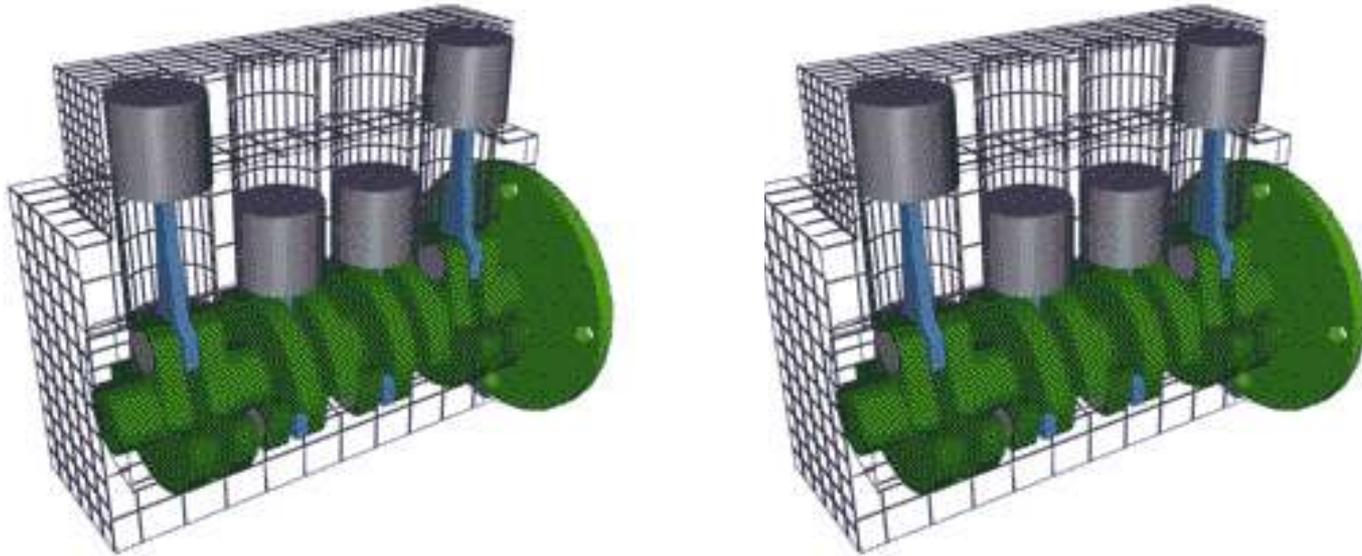
Deployment



John Streufert (DOSCISO@state.gov)
Deputy Chief Information Officer for Information Security
US Department of State

Blocks For The Engine of Transformation

Paradigm Shift(s)



**Approach Balance/tune essential
elements now in operation**

Cylinder # 1: Change

- Business/Organization critical success factors:
 - Business Change Management
 - Communications
 - Culture of Cost Effectiveness
 - Negotiation
 - Security Risk/Threat Analysis
 - Performance Measurement
 - Data Analysis

Cylinder #2: Technical

- Critical Success Factors (Technical):
 - Data Enclave Protection
 - ID & Authentication
 - Data Mining Tools: Interface Design and Construction
 - Database design/administration/hardening
 - Information Broker management
 - System Administration



Cylinder #3: Adequacy of Plan

Coverage of CAG

See Next Page

CAG ID	Consensus Audit Guidelines	NIST-800-53	CIRT Events 11 mo
1	Inventory of authorized and unauthorized hardware	CM-1, CM-2, CM-3, CM-4, CM-5, CM-8, CM-9	Multiple Tools < 6% < 22%
2	Inventory of authorized and unauthorized software	CM-1, CM-2, CM-3, CM-5, CM-7, CM-8, CM-9, SA-7	
3	Secure configurations for HW and SW, if available	CM-6, CM-7, CP-10, IA-5, SC-7	Nominal
4	Secure configurations for network devices such as firewalls and routers	AC-4, CM-6, CM-7, CP-10, IA-5, RA-5, SC-7	Nominal
5	Boundary Defense	AC-17, RA-5, SC-7, SI-4	< 7%
6	Maintenance/Analysis of complete security audit logs	AU-1, AU-2, AU-3, AU-4, AU-6, AU-7, AU-9, AU-11, AU-12, CM-3, CM-5, CM-6, SI-4	Nominal
7	Application software security	AC-4, CM-4, CM-7, RA-5, SA-3, SA-4, SA-8, SA-11, SI-3	Decentralized
8	Controlled use of Administrative Privileges	AC-6, AC-17, AT-2, AU-2	Nominal
9	Controlled access based on need to know	AC-1, AC-2, AC-3, AC-6, AC-13	< 1%
10	Continuous vulnerability testing and remediation	CA-2, CA-6, CA-7, RA-5, SI-2	Nominal
11	Dormant account monitoring and control	AC-2, PS-4, PS-5	Nominal
12	Anti-malware defenses	AC-3, AC-4, AC-6, AC-17, AC-19, AC-20, AT-2, AT-3, CM-5, MA-3, MA-4, MA-5, MP-2, MP-4, PE-3, PE-4, PL-4, PS-6, RA-5, SA-7, SA-12, SA-13, SC-3, SC-7, SC-11, SC-20, SC-21, SC-22, SC-23, SC-25, SC-26, SC-27, SC-29, SC-30, SC-31, SI-3, SI-8	< 60%
13	Limitation and control of ports, protocols and services	AC-4, CM-6, CM-7, SC-7	Not yet graded
14	Wireless device control	AC-17	Nominal
15	Data leakage protection	AC-2, AC-4, PL-4, SC-7, SC-31, SI-4	Pending

Cylinder #4: Logistics

Tools to Deploy:

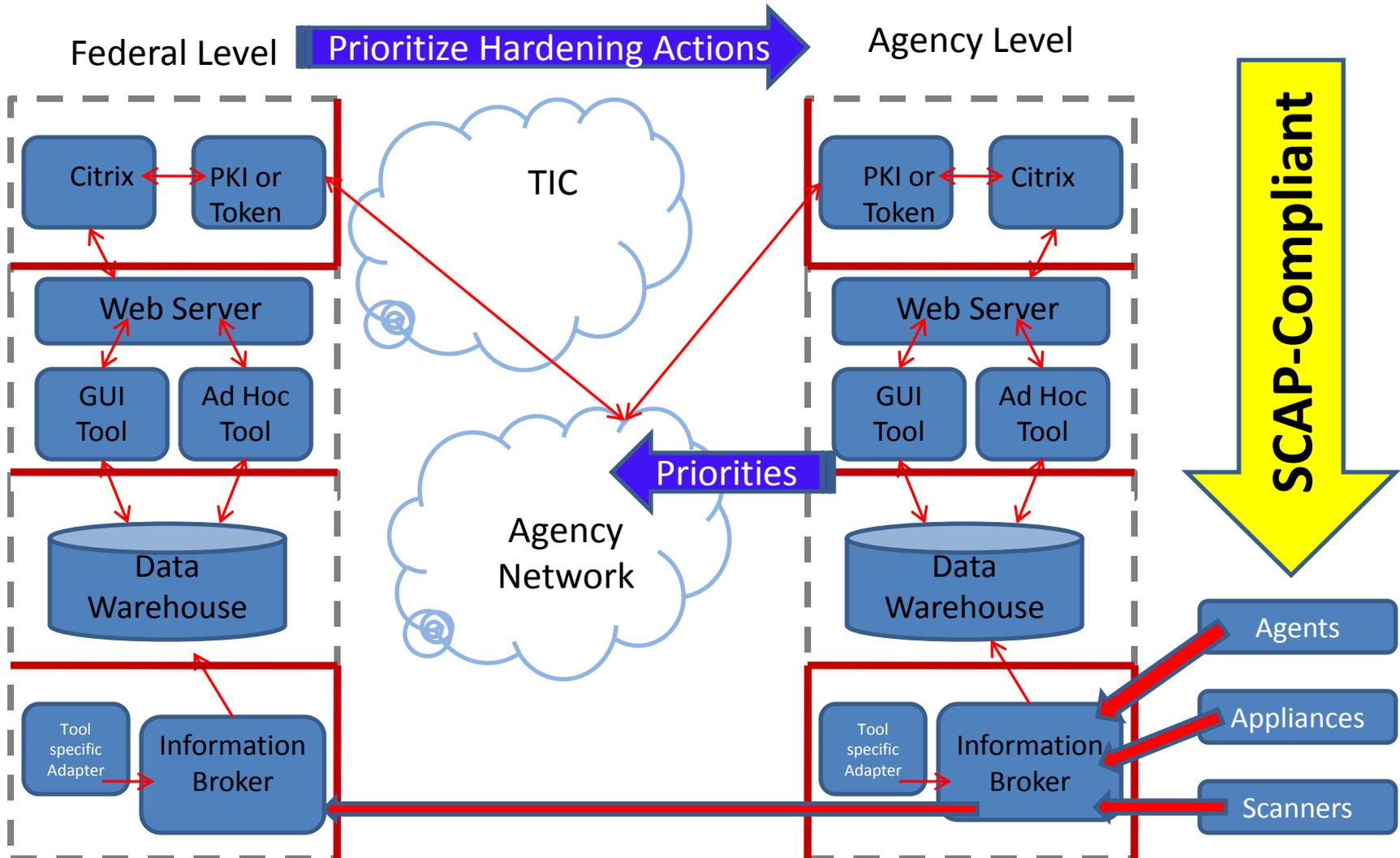
1. CAG Directed Toolset – baseline growing to 15 control families. Status now:
 - a. SMS (Systems Management Server – Microsoft)
 - b. Vulnerability/Configuration Management
 - N-Circle, Tenable, McAfee
2. Data warehouse to store enterprise risk information securely (GOTS)
3. Risk Scoring Dashboard (GOTS)

Cylinder #5: Acquisition

Model:

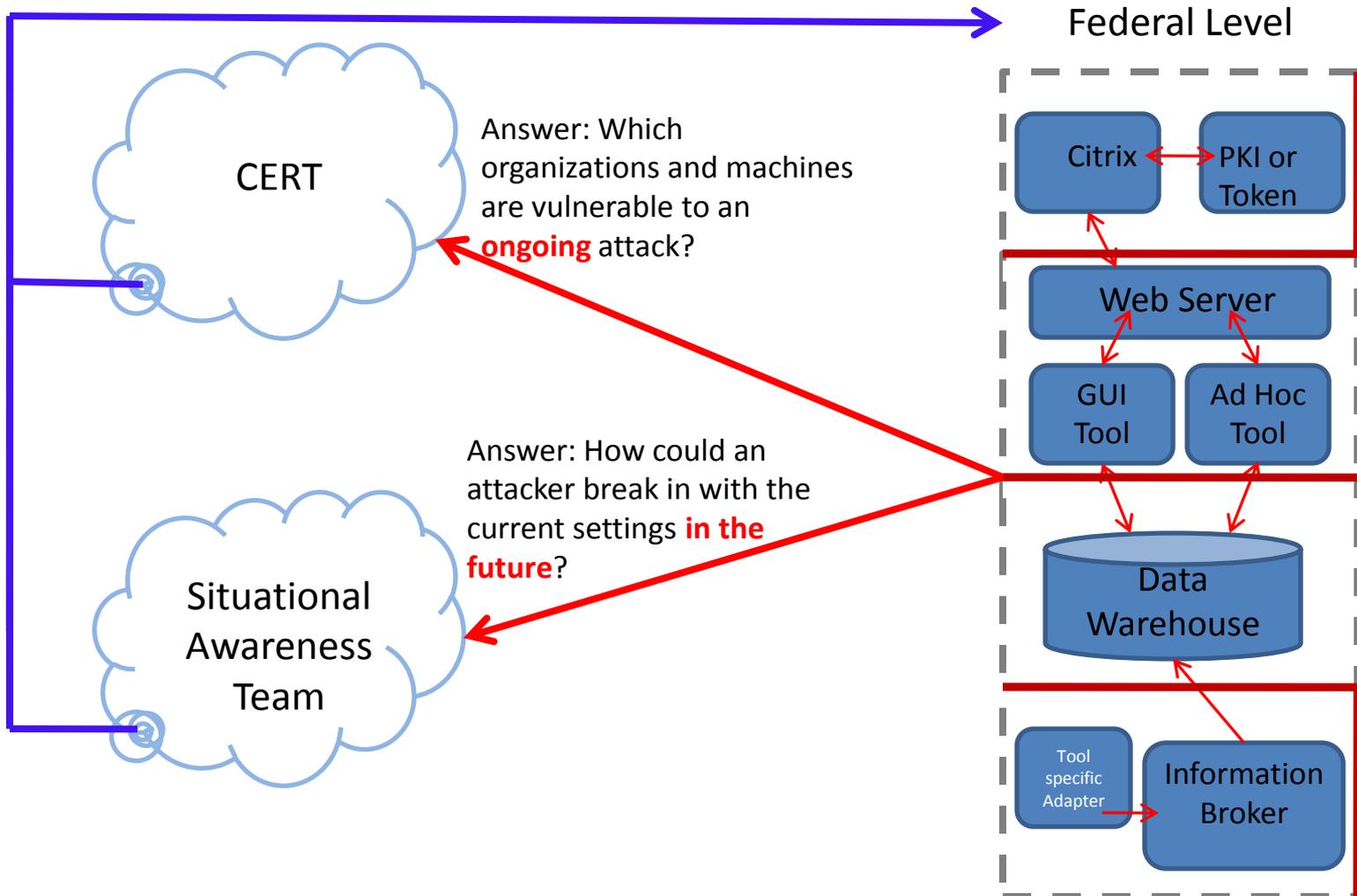
- Multiple award contract from GSA
 - Dashboard, 15 tool groups, data integration
 - Continuous update of scanner technology
- OMB, DHS, NIST guidance to protect .gov
 - Yardsticks needed for each of 20 CAG elements
 - Public-private FDCC model achieved the most, the fastest;
- Federal level interdisciplinary support team

Cylinder #6: Architecture



Cylinder #7: Integration

Answer: Adjust priorities for hardening in response to actual/possible threats



Cylinder #8 Training

Tips of the Day Application

Security Tip of the Day [options](#) [help/comment](#)



Is your classified media “secured?”

Removable hard drives containing classified information must be locked in an approved safe after you finish using them!

Classified media aren’t “secured” until they are locked in an approved safe.

If I leave my computer for any reason, I must secure all removable media that contain CLASSIFIED information.

[view my results](#)