

Measure More, Spend Less *ON THE WAY TO* Better Security



John Streufert
Chief Information Security Officer
US Department of State
November 12, 2009

\$1B Question

For DoS subset, case study show:

- **How attacks are changing**
- **Not FISMA law, but implementation**
- **How C&A costs were reduced 62%**
- **How C&A money saved allowed for higher ROI, continuous monitoring, and new, broad based efficiencies in defensive cyber security operations**

**Attacks
Increasing**

Increase & Shift

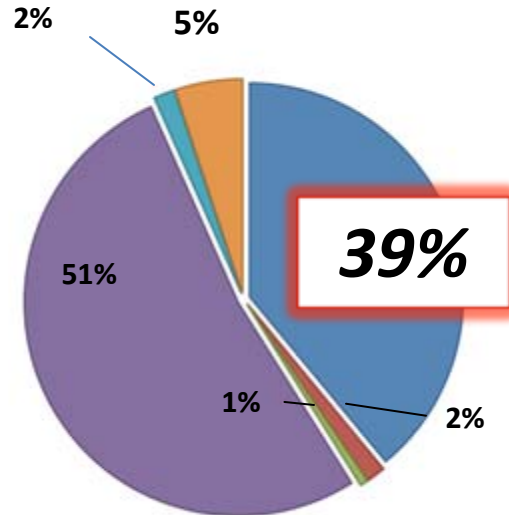
TICKETS

Years Compared	
<i>FY 08</i>	<i>FY 09</i>
2104	3085

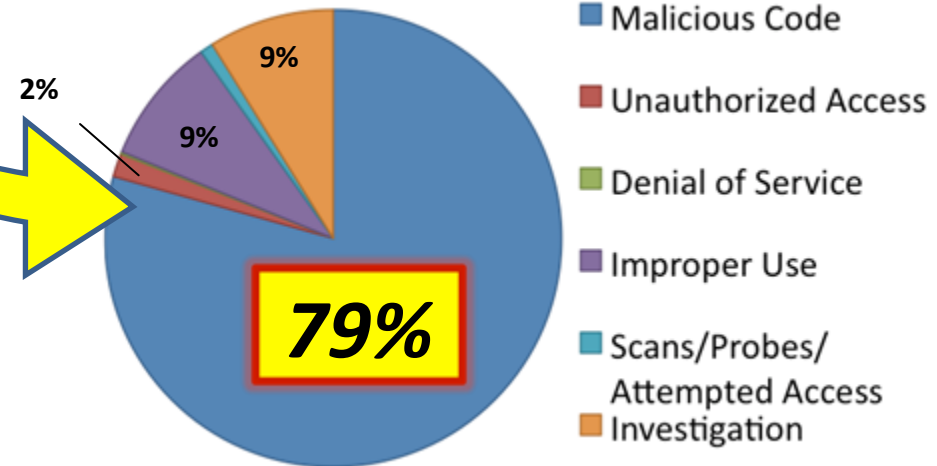
FY 09 Quarters	
<i>Quarters</i>	<i>Tickets</i>
Oct-Dec 08	560
Jan-Mar 09	555
Apr-Jun 09	639
July-Aug 09 <i>(Partial)</i>	805

Months Compared		
	<i>2008 - Tickets</i>	<i>2009 - Tickets</i>
June	154	300
July	183	352
August	250	453

FY08



FY09



TYPE

Targets:

[11 months before Feb 09]

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	+ 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%

Penetration Tests

80% of the successful attacks used known vulnerabilities

Law and Regulation

One Word

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 House Oversight and Government Reform website

FISMA 1.0

Compliance “*SNAPSHOTS*”

1. “**Annual**” awareness course
2. “**Annual**” systems inventory
3. “**Annual**” testing
4. C&A[⌘] every “**three**” years
5. Weaknesses “**Quarterly**”
6. **Configuration Management**
7. **Incident Reporting**

⌘

Certification and Accreditation studies

CASE STUDY

Department of State

- 70,000 people
- 260 overseas & 40 CONUS locations
- Staff with significant IT security responsibilities : **4135**
- Staff doing C&A: **60**

USAID (FY 2003 +)

- 8000 people
- 72 overseas locations



Concerns: FY2007

- **Material weakness: Teaming**
- **Cost of compliance program**
- **FISMA: Four F's , One D Minus**
- **Large numbers of vulnerabilities**

C&A PROCESS

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. CISO's control few systems directly, but are accountable.
- f. C&A's focus on individual systems. Enterprise faces risk.
- g. Many attacks focus on subset of controls (CAG)

Targeted Gains

C&A cost down 56% then 62% ✕

- Invest in tool kits for everything

✕ Certification & Accreditation decentralized, just in time

Technical control data efficiency:

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

Assemble accountable tiger teams:

- inventory and to reduce site risks

FISMA + Pilot

Continuous:

7. Incident Reporting
6. Configuration Management
5. Weakness updated “daily”
4. C&A technical control (x72) ✕
3. Daily not “Annual” testing
2. Inventory improvements
1. “Daily” awareness training

✕

Certification and Accreditation study of technical controls

Risk Scoring Initiative



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

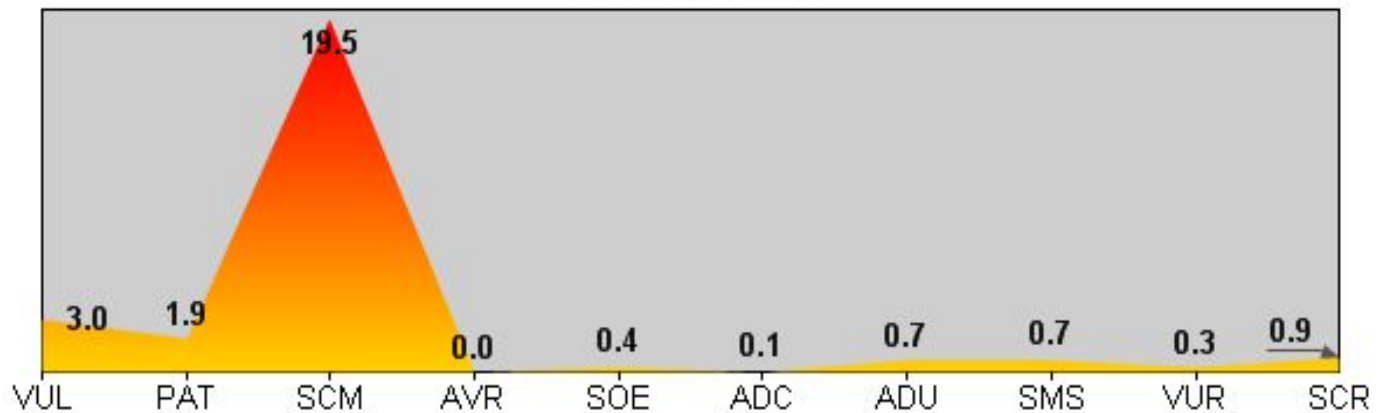
Risk Score Advisor






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-

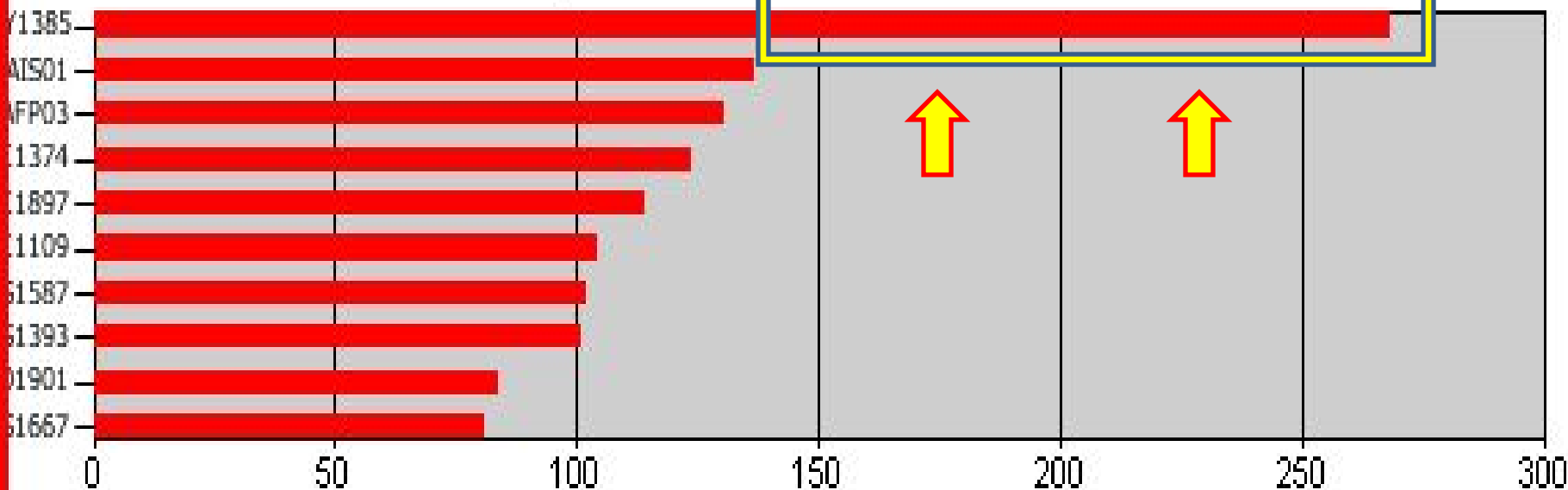
Risk Score Profile



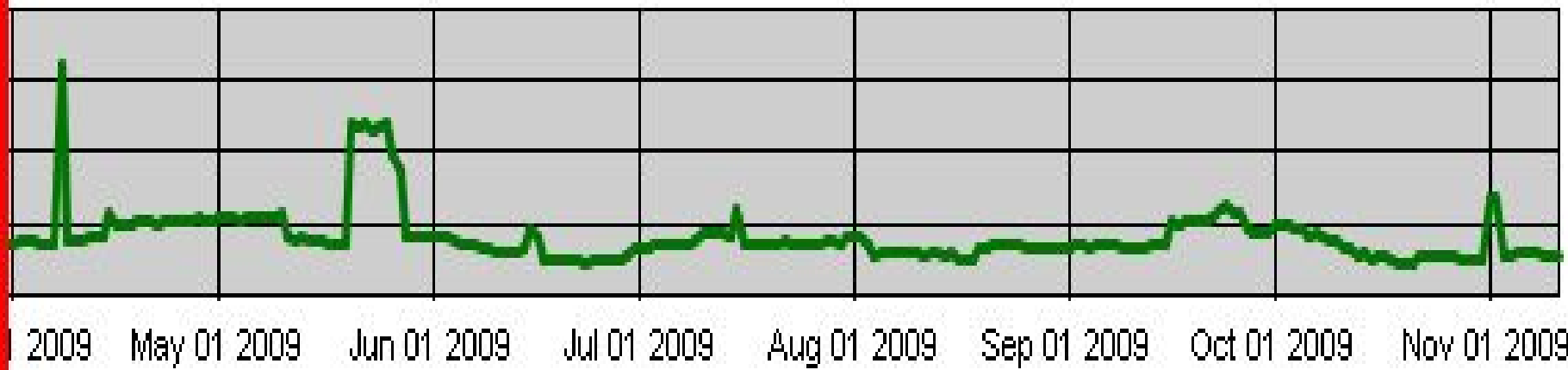
Component	Risk Score	Avg / Host	% of Score	How Component is Calculated
VUL - Vulnerability 	947.0	3.0	10.9 %	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
PAT - Patch	603.0	1.9	6.9 %	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
SCM - 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 % 	

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





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

- E** [All Risk Scoring Exceptions](#)
Enterprise Level
Enterprise and local risk scoring exceptions.
- E** [Enterprise Risk Score Monitor](#)
Enterprise Level
Risk scores, grades, and rankings for each primary site in the Enterprise
- E** [Site Collection Risk Score Monitor](#)
Enterprise Level
Risk scores, grades, and rankings for each site in a named site collection
- E** [Vulnerability Management](#)
Enterprise Level
Active scoring exceptions for vulnerabilities
- R** [Regional Risk Score Monitor](#)
Regional Level
Risk scores, grades, and rankings for each site
- S** [Risk Score Advisor](#)
Site Level
Analysis assistance to facilitate improvement of risk score
- S** [Risk Score Rank](#)
Site Level
Displays site risk score ranks in the enterprise
- S** [Risk Scoring Exceptions](#)
Site Level
Risk scoring exceptions applicable to the selected site



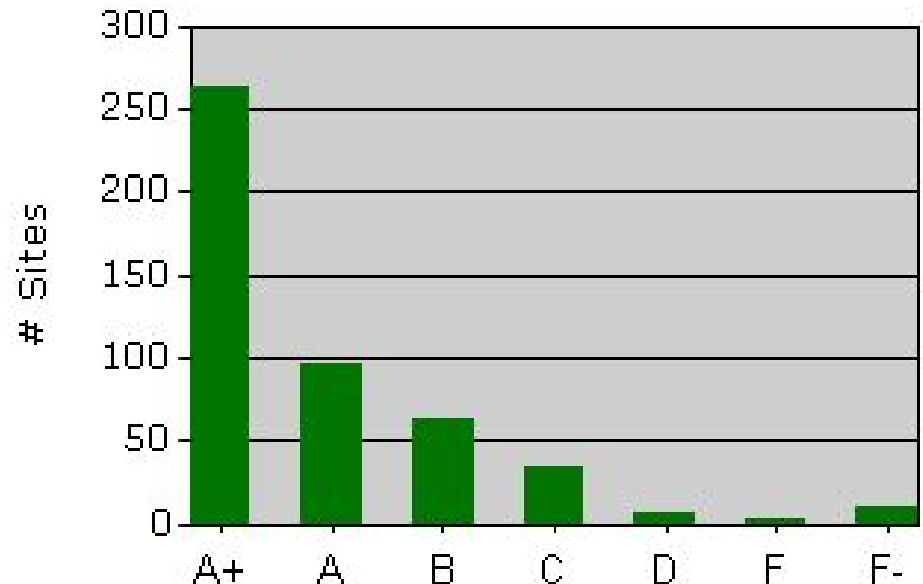
Risk Score Monitor Enterprise

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

Grading Scale

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-

Grade Dis



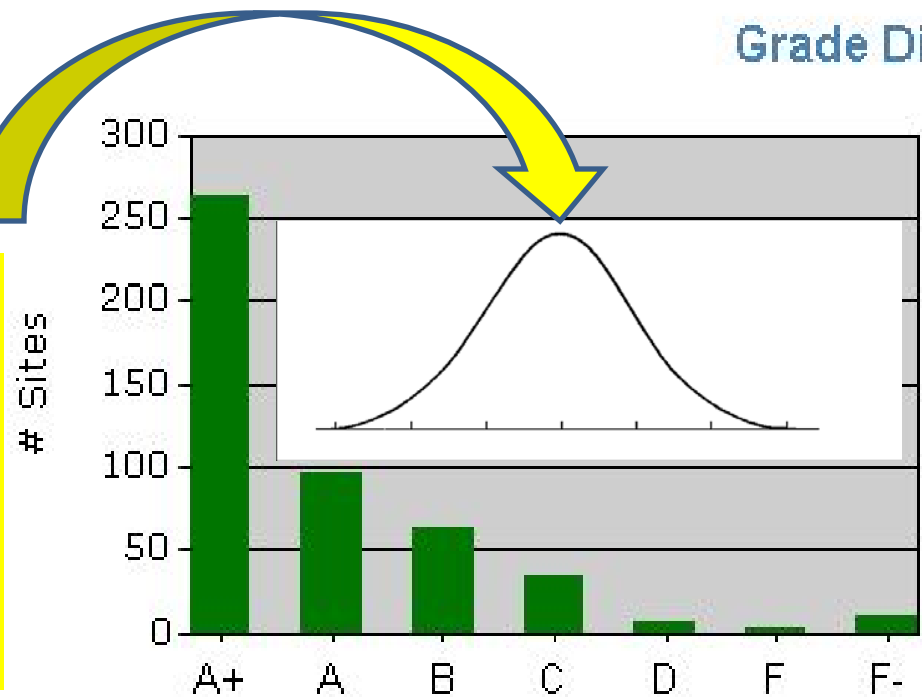
Risk Score Monitor Enterprise

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

Grading Scale

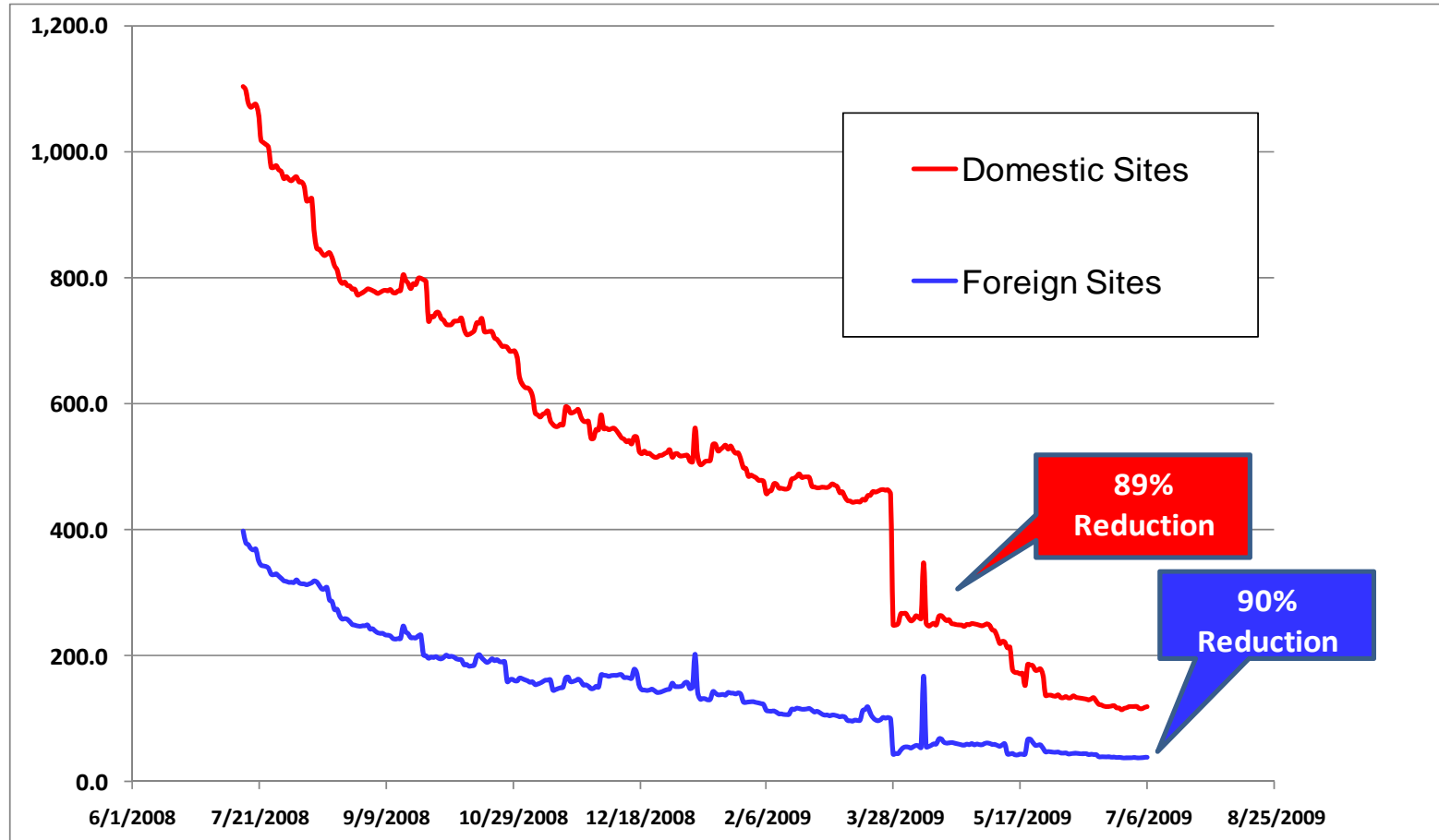
Average Risk Score			Grade	# Sites
At Least	Less Than			
0.0	40.0		A+	13
40.0	75.0		A	25
75.0	110.0		B	36
110.0	180.0		C	60
180.0	280.0		D	93
280.0	400.0		F	133
400.0	-		F-	

Grade Dis





Results in 12 Months



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

Federal conclusions

- Concepts are scalable to large complex public (and possibly) private sector organizations
- Spending of \$1.3 billion estimated for federal C&A cycle:
 - Higher ROI for continuous monitoring of technical controls as a substitute for paper reports
- Progress in reducing vulnerabilities on a summary level could be fed to Cyber Scope

Additional slides

Essential Elements to Begin

Key Pieces:

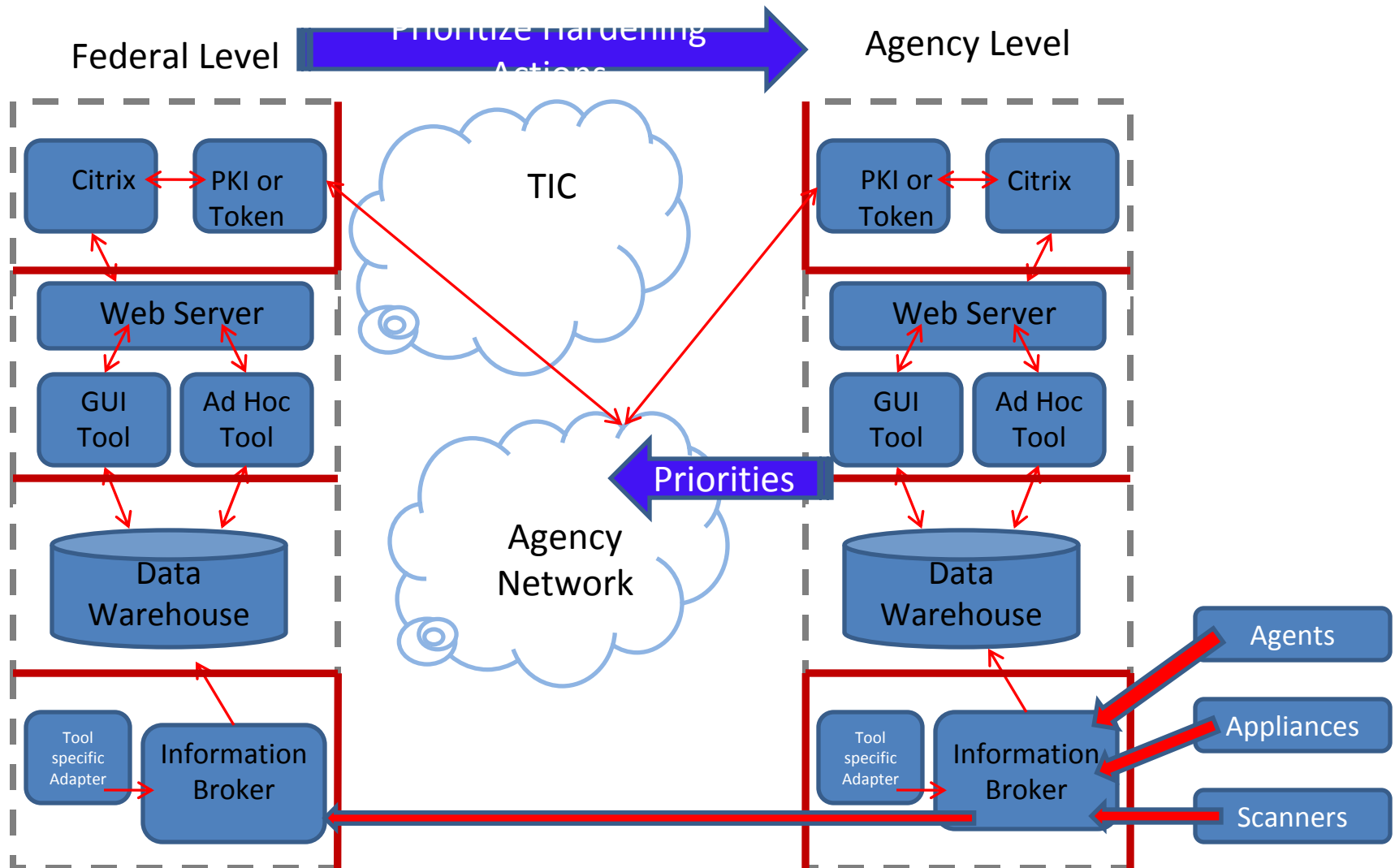
1. CAG Directed Toolset – baseline growing to 15 control families. Status now:
 - a. SMS (Systems Management Server – Microsoft)
 - b. Vulnerability/Configuration Management
 - N-Circle, Tenable, McAfee
2. Data warehouse to store enterprise risk information securely (GOTS)
3. Risk Scoring Dashboard (GOTS)

Wider Implementation

Recommended 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
- DHS/DoD provide protection for data

Security Dashboard Architecture



Security Dashboard: Other Uses of Data

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

