Leveraging FISMA Guidance to Support an Effective Risk Management Strategy to Secure IT Systems and Meet Regulatory Requirements.

Thomas Chimento Ph.D., CISSP, CCE, CISA
Product Manager
Webroot Software

Bill Robinson, CISSP, IAM
Senior Information Security Consultant
SecureInfo Corporation

What is FISMA?

- FISMA requires each federal agency to *"**develop, document, and implement** an agency-wide information security program … to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source."*

FISMA Requirements

- **At a high level, FISMA requires agencies to:**
  - Plan for security
  - Ensure that appropriate officials are assigned security responsibility
  - Review the security controls in their information systems
  - Authorize system processing prior to operations and, periodically, thereafter

FISMA Requirements

- Periodic assessments of risk,
- Policies and procedures that are based on risk assessments,
- Security awareness training
- Periodic testing and evaluation
- A process to address deficiencies
- Procedures for detecting, reporting, and responding to security incidents
- Plans and procedures to ensure continuity of operations

The NIST Responsibilities under FISMA

- Standards to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels and impact levels
- Guidelines recommending the types of information and information systems to be included in each category
- Minimum information security requirements, (i.e., management, operational, and technical security controls), for information and information systems in each such category

NIST documents for FISMA

- Guide for the Security Certification and Accreditation of Federal Information Systems (SP 800-37)
- The Guide for Developing Security Plans for Information Technology Systems (SP 800-18)
- Standards for Security Categorization of Federal Information Systems (FIPS 199)
- Guide for Mapping Types of Information and Information Systems to Security Categories (SP 800-60)
- Minimum Security Controls for Federal Information Systems (FIPS 200)
- Recommended Security Controls for Federal Information Systems (SP 800-53)
- Guide for Assessing the Security Controls in Federal Information Systems (SP 800-53A)

Guide for the Security Certification and Accreditation of Federal Info Systems (SP 800-37)

- Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system
- It determines the extent to which the controls are:
  - Implemented correctly
  - Operating as intended
  - Producing the desired outcome with respect to meeting the security requirements for the system
- Security **certification** is a technical process while system **accreditation** is a management function

The Guide for Developing Security Plans for Information Technology Systems (SP 800-18)

- Describes NIST's view of the system analysis process
- Provides guidance on the general information contained in all security plans
- Defines the concept and function of the three security control categories:
  - Management Control
  - Operational Controls
  - Technical Controls
- Provides examples of system "rules of behavior" and a template for security plans

The Standards for Security Categorization of Federal Information Systems (FIPS 199)

- Sets out the standards for categorizing information and information systems
- Security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals
- Security categories are used in conjunction with vulnerability and threat information in assessing the risk to an organization

FIPS 199 Impact Levels

- FIPS 199 defines three levels of potential impact on organizational operations, assets or individuals resulting from the loss of confidentiality, integrity, or availability:
  - **LOW** if the loss of is expected to have a **limited** adverse effect
  - **MODERATE** if the loss is expected to have a **serious** adverse effect
  - **HIGH** if the loss is expected to have a **severe or catastrophic** adverse effect

The Guide for Mapping Types of Information and Information Systems to Security Categories (SP 800-60)

- Designed to help organizations map security impact levels in a consistent manner
- Defines relationships between:
  - Types of information (e.g., privacy, medical, proprietary, financial, trade) and
  - Information systems (e.g., mission critical, mission support, administrative)
- Divided into two volumes
  - Volume I: guidelines for information type identification and security categorization
  - Volume II: appendices, including examples of impact assignments and security categorization rationale

FIPS 200

- **Provides Control Selection Guidance**
  - Technology-related considerations
  - Common security control-related considerations
  - Public access information systems-related considerations
  - Infrastructure-related considerations
  - Scalability-related considerations
  - Risk-related considerations

Recommended Security Controls for Federal Information Systems (SP 800-53)

- **Security controls possess two important properties:**
  - **Robustness –** the property that allows security controls to be defined with varying strengths of function and with varying degrees of assurance regarding the effectiveness of implementation
  - **Flexibility** – the property allows organizations to tailor security controls to satisfy unique security policies and to meet specific operational needs

Security Control Organization

CLASS	FAMILY	IDENTIFIER	# OF CONTROLS
Management	**Risk Assessment**	**RA**	**5**
Management	**Planning**	**PL**	**5**
Management	**System and Services Acquisition**	**SA**	**11**
Management	**Certification, Accreditation, and Security Assessments**	**CA**	**7**
Operational	**Personnel Security**	**PS**	**8**
Operational	**Physical and Environmental Protection**	**PE**	**17**
Operational	**Contingency Planning**	**CP**	**10**
Operational	**Configuration Management**	**CM**	**7**
Operational	**Maintenance**	**MA**	**6**
Operational	**System and Information Integrity**	**SI**	**12**
Operational	**Media Protection**	**MP**	**7**
Operational	**Incident Response**	**IR**	**7**
Operational	**Awareness and Training**	**AT**	**4**
Technical	**Identification and Authentication**	**IA**	**7**
Technical	**Access Control**	**AC**	**20**
Technical	**Audit and Accountability**	**AU**	**11**
Technical	**System and Communications Protection**	**SC**	**19**

Control Selection Table

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
Access Control				
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-9	Previous Logon Notification	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10

A Sample Control

AU-3 Content of Audit Records

- **Control**: The information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.

- **Supplemental Guidance**: Audit record contents includes, for most audit records: (i) date and time of the event; (ii) information system location of the event; (iii) type of event; (iv) subject identity; and (v) the outcome (success or failure) of the event

- **Control Enhancements**:
  (1) The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.
  (2) The information system provides the capability to centrally manage the content of audit records generated by the individual components throughout the system.

Guide for Assessing the Security Controls in Federal Information Systems (SP 800-53A)

- **Establishes methods and procedures to assess security controls**
- **Provides guidance on:**
  - Assessment methods and procedures
  - Interviewing personnel associated with the security aspects of the system
  - Reviewing and examining security-related policies, procedures, and documentation
  - Observing security-related activities and operations
  - Analyzing, testing, and evaluating the security relevant and security critical aspects of system hardware, software, firmware, and operations
  - Conducting demonstrations and exercises

A Sample Control Assessment

step	Assessment Procedure	L	M	H
AU-3.1	**Examine** organizational records or documents to determine if the info system audit records capture sufficient information to establish what events occurred, the sources of the events and the outcomes of the events	*	*	*
AU-3.2	**Test** the content of the audit records by attempting to perform actins that are configured to generate audit records to determine if the audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events		*	*
AU-3.4	**Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if the info system consistently captures sufficient audit information to support organizational audit and accountability requirements on an ongoing basis			*

Summary and Conclusions

- The NIST Information Security Governance framework provides cost effective security through:
  - The tight coupling of the security architecture to business requirements (mission)
  - Emphasizing a risk-based approach to control selection
- The framework can be adopted and adapted by all sizes of government agencies and private sector enterprises
- It encourages taking a step back to look at the “big picture” with respect to how information security enables business processes and protects the enterprise
- It does so without sacrificing the level of granularity of guidance that it takes to “make the rubber meet the road”
- It’s in the public domain!

Overview

- C&A Challanges
- State of Affairs
  - 10 Successful Steps
- Case Studies
- Lessons Learned
  - 10 Pitfalls to Avoid

The C&A FISMA Challange

FEDERAL COMPUTER SECURITY REPORT CARD			April 12, 2007		
GOVERNMENTWIDE GRADE 2006: C-					
	2006	2005		2006	2005
AGENCY FOR INTERNATIONAL DEVELOPMENT	A+	A+	DEPARTMENT OF ENERGY	C-	F
HOUSING AND URBAN DEVELOPMENT	A+	D+	DEPARTMENT OF HOMELAND SECURITY	D	F
NATIONAL SCIENCE FOUNDATION	A+	A	NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	D-	B-
OFFICE OF PERSONNEL MANAGEMENT	A+	A+	DEPARTMENT OF AGRICULTURE	F	F
GENERAL SERVICES ADMINISTRATION	A	A-	DEPARTMENT OF COMMERCE	F	D+
SOCIAL SECURITY ADMINISTRATION	A	A+	DEPARTMENT OF DEFENSE	F	F
DEPARTMENT OF JUSTICE	A-	D	DEPARTMENT OF EDUCATION	F	C-
ENVIRONMENTAL PROTECTION AGENCY	A-	A+	DEPARTMENT OF THE INTERIOR	F	F
SMALL BUSINESS ADMINISTRATION	B+	C+	NUCLEAR REGULATORY COMMISSION	F	D-
DEPARTMENT OF HEALTH AND HUMAN SERVICES	B	F	DEPARTMENT OF STATE	F	F
DEPARTMENT OF TRANSPORTATION	B	C-	DEPARTMENT OF TREASURY	F	D-
DEPARTMENT OF LABOR	B-	A+	DEPARTMENT OF VETERANS AFFAIRS**	--	F

**The Department did not provide its FY06 FISMA Report

FCWCOM

Diane Frank
A study of lessons learned from the Federal Information Security Management Act (FISMA) seems to pinpoint certification and accreditation (C&A) as the most important aspect of compliance.

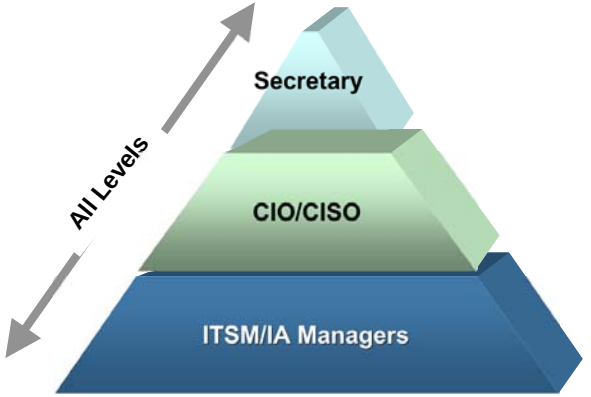
While several improvements have been made, agency reports reveal areas requiring strategic and continued management attention over the coming year;

Quality of certification and accreditation process.
OMB encourages agency CIOs and IGs to work together to improve the quality of the agency's C&A process, and uses the IGs independent assessment of this process as one factor in assessing an agency's status and/or progress on the President's Management Agenda scorecard.

Step 1

Establish C&A Management Commitment/Expectations

- Must be a Visible Priority from the Top
- Consistent and Committed Communication
- Metrics and Reporting
- Well established standards



Engagement At All Levels

Step 2

Identify C&A System Inventory and Boundaries

- Inventory all Major Applications and General Support Systems
- Define System Boundaries
- Identify applicable Data Owners
- Determine FISMA Reportable Systems Subset
  - Mission Critical
  - Office Automation

Focus, Speed, Quality & Value

Step 3

Determine System Accreditation Status

- How many systems have a ***current*** accreditation decision?
- Which systems have an Approval to Operate for 1 year or more?
- Which systems have an ***Interim*** Approval to Operate?
- How many will ***expire*** within the next 180 days?

Step 4

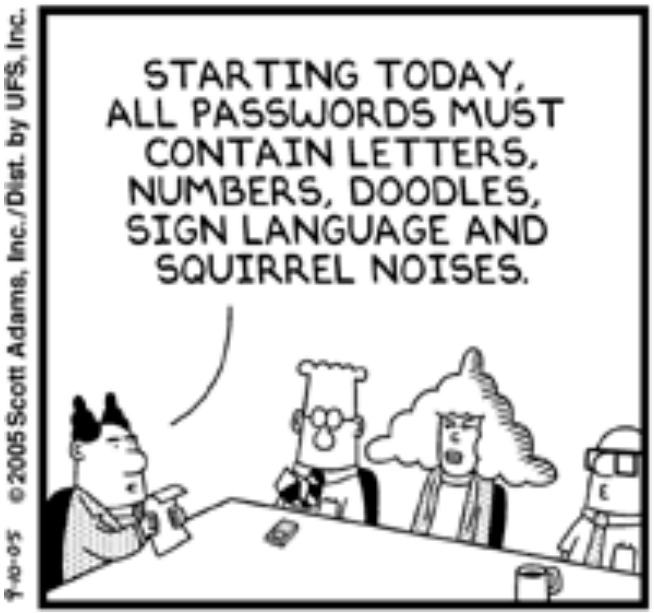
Determine Level of Effort

- Low – Moderate – High
- Biggest Bang for the Buck
- What Systems Must be Done - ***No Matter What***?
- Which Systems are Due for Termination?

Step 5

Promote C&A Communication

- Regular
- Consistently across all levels
- Presentations, Conferences/Seminars
- Awareness Campaigns
- Internal & External



Step 6

Develop Management Strategy for Completion

- Know Where You Are Today
- Existing process on track?
- Establish Practical, Measurable, and Attainable Metrics/Goals
- Build a business case for success
- Formalized & Tracked - CCB

Feedback Essential for Success

Step 6 (cont)

Pre-Requisites to Build a Business Case

- Number of C&A's to Perform
- Available Budget $$
- Available Resources
- Ability to Train
- Geographical Locations
- C&A Improvement Priority
- ROI that Counts (Speed, Quality & FISMA grade)

Step 7

Create Support Structure

- Develop support teams
  - Trained?
  - Available?
- Automated Tools
  - C&A Collaboration Tool
  - FISMA Reporting
  - Scanning Tools
- Outsourcing
  - Well established, ability to scale, Proven track record

Step 7 (cont)

Training

- Key Success Factor
- Must Target All Levels
- Comprehensive…But…Walk Before They Run
  - Pre-Sell/Education: Webex, Onsite, Lunch & Learn
  - CBT Training, Flash, Mailings, Handouts
  - Process and Product Training
  - Elementary/Overview: Accelerator Workshop
  - Advanced User Training

User Adoption is Key

Step 7 (cont)

Consider Automation

- ***Manual –*** *Slow, Time Consuming, Resource Intensive, Expensive*
- ***Quality –*** *Inconsistent, Ad Hoc*
- ***Requirements –*** *Which Ones Apply? How To Keep Updated?*
- ***Documentation –*** *Which Ones? How To Complete?*
- ***Management –*** *Difficult to Delegate and Control*
- ***Reporting Burden –*** *OMB and FISMA*

FISMA

POA&M Data Calls

C&A Process (Artifacts, ST&E)

Step 8

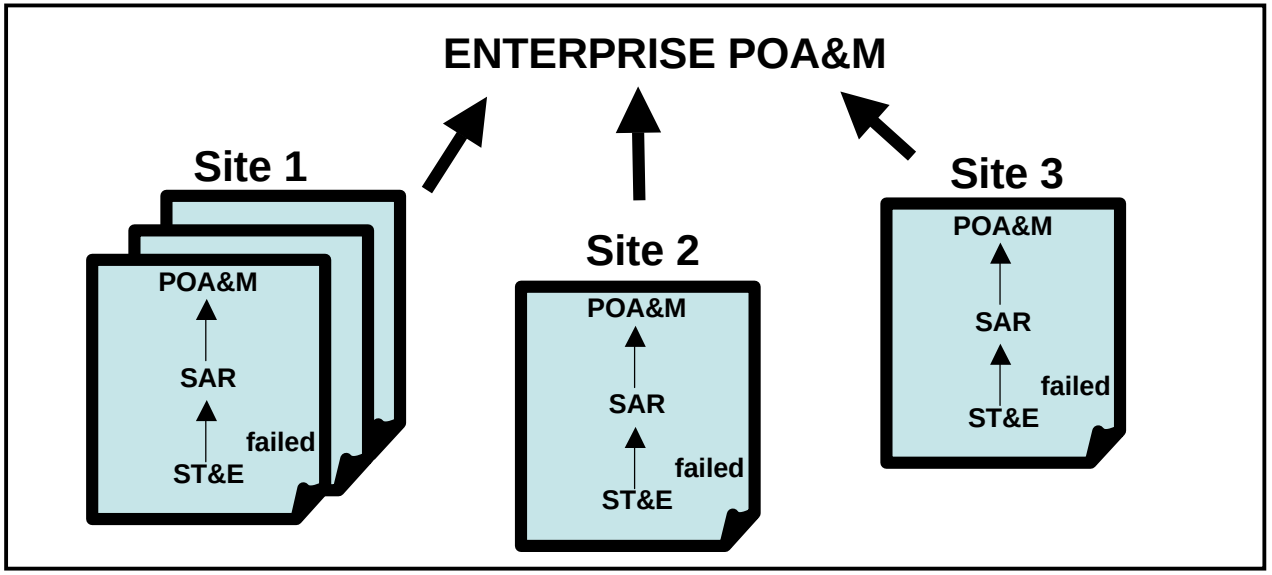
Identify Common Security Issues.

- Common Inherited Controls
- Standardized Security Procedures
- Determine Weakest Link to System
- Analyze Security Assessment Results

Step 9

Develop a Plan of Action and Milestones

- Typical Data Calls Not Locked to C&A's/ST&E/SAR
- No Facilitated Tracking, Reporting or Auditability



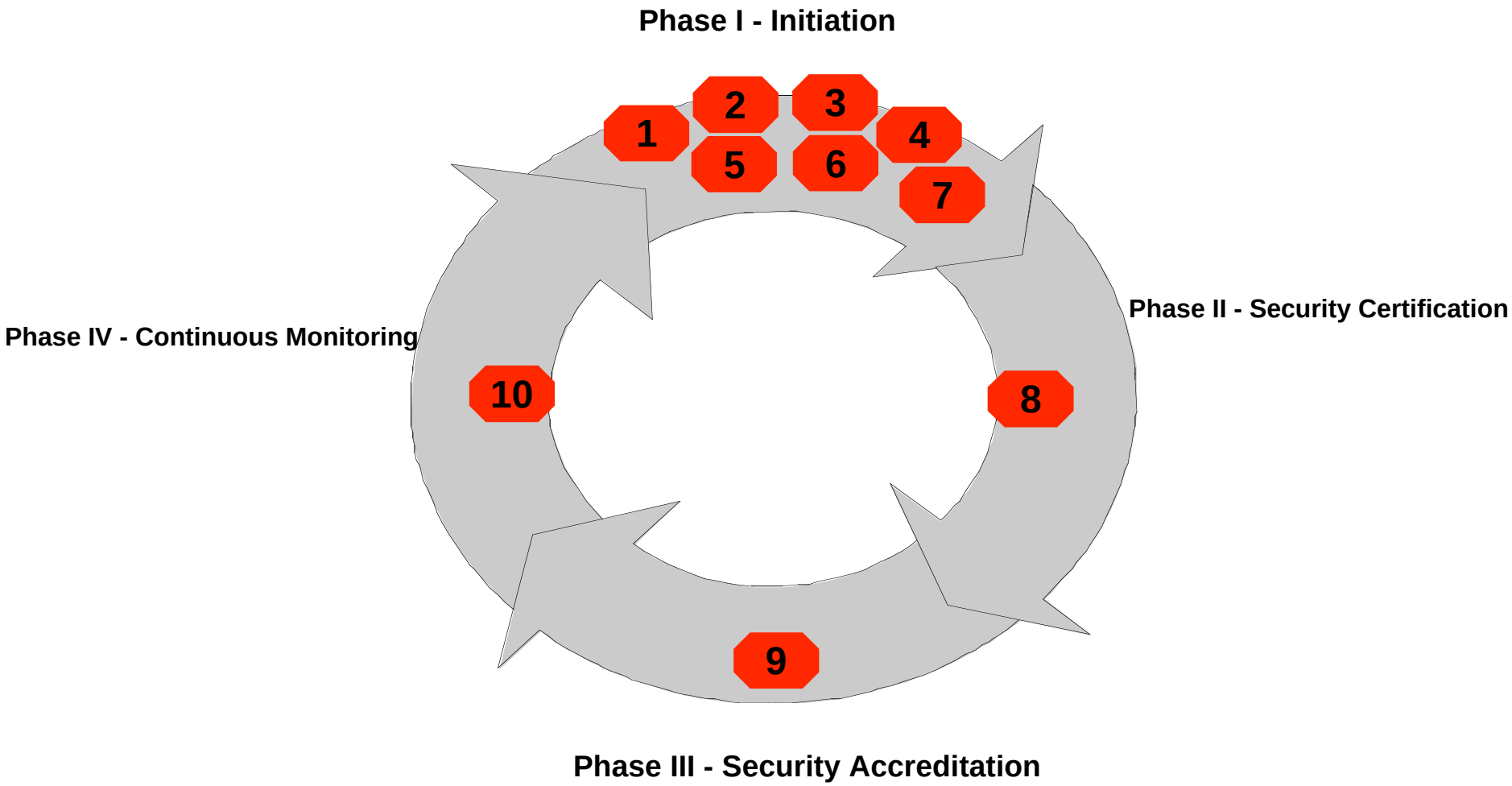
Put Teeth in Process & Hold People Accountable

Step 10

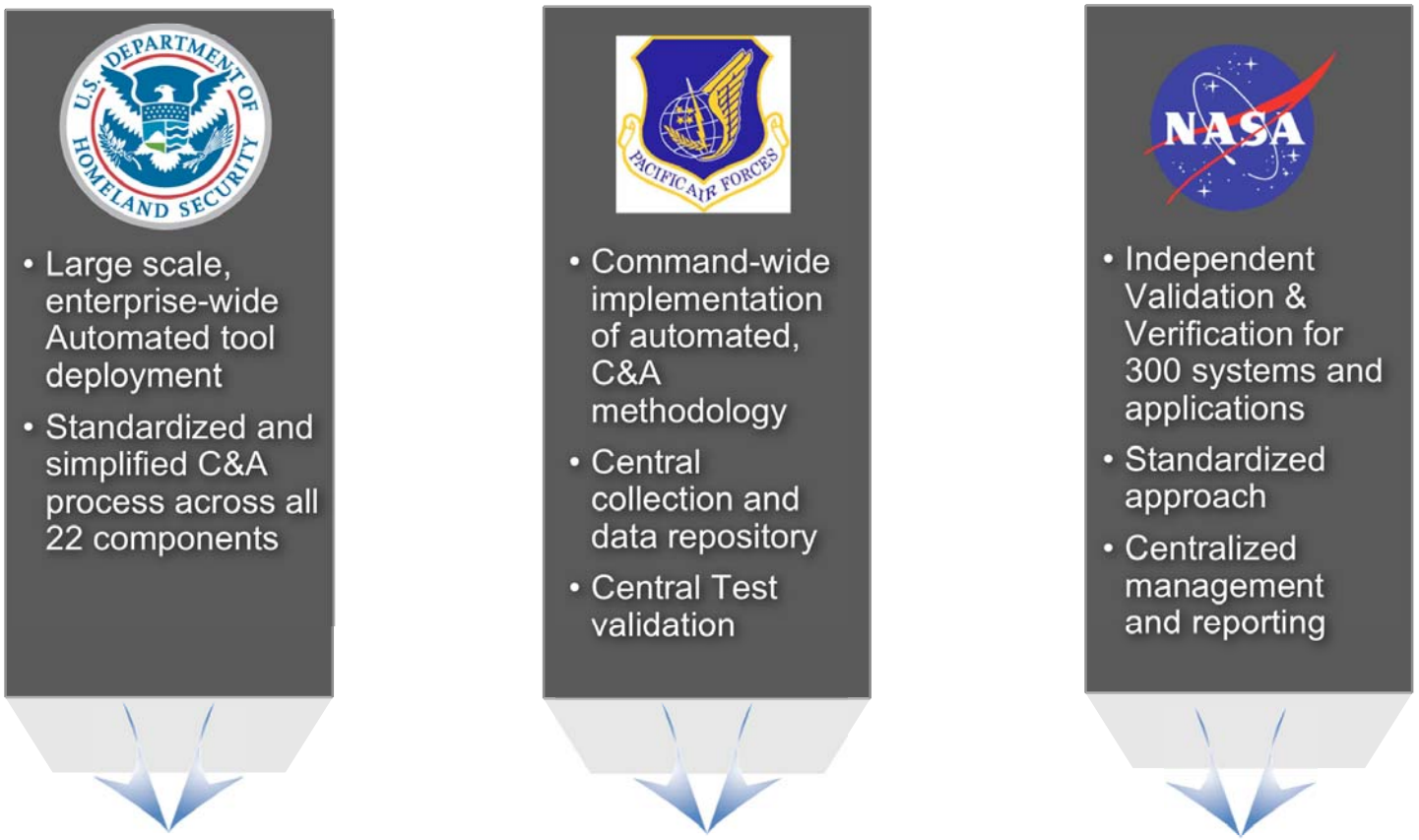
Roadmap to Success

- Fine Tune the C&A Plan
- Strengthen Commitment at all Levels
- Communicate on Recurring Basis
- Maintain Configuration Control
- Consider Automation as needed
- Train, Train, Train
- Centralized POA&M Reporting
- Management Updates/Reporting

When do I do these steps?



Case Study Overview



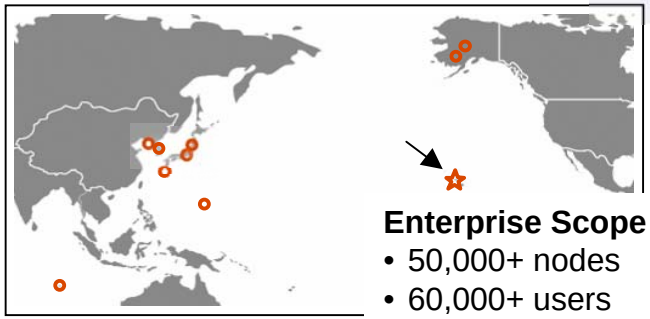
Managing and maintaining comprehensive C&A programs

Pacific Air Forces – Case Study

PACAF's primary mission is to provide ready air and space power to promote U.S. interests in the Asia-Pacific region during peacetime, through crisis, and in war.

Challenge

- Certification & Accreditation (C&A) of the PACAF NIPRNet/SIPRNet backbone
- C&A of all other PACAF systems/networks
- Maximize existing resources
- Standard methodology for C&A of PACAF systems
- Command-wide view of C&A status



Enterprise Scope

- 50,000+ nodes
- 60,000+ users
- 10 Bases throughout Pacific Rim
- 3 million+ intrusion attempts/year

Solution

- Contracted on-site enterprise-wide IA support using automated tool- RMS
- Command-wide implementation of automated, standardized C&A methodology
- Reduced costs through 40% savings in time performing C&As
- Centralized solution provides ready access to standardized, high quality C&A packages for management reporting and Inspector General audits

DHS –Case Study

- **Challenge**
- Diverse organization of 22 agencies and 180,000 employees
- Varying levels of component security maturity and processes
- No master, validated systems inventory
- System boundaries not well defined

Solution

- Dramatically improved # of certified systems
  - 95% in 2006 from 22% in 2005
- Standardized C&A baseline
  - NIST–based, DHS specific policies (DHS 4300)
- Enforced security baseline
  - C&A enables process standardization
- Compiled complete, accurate inventory
  - All DHS systems defined by a C&A boundary
- Centralized FISMA reporting
  - Hundreds of systems across all DHS agencies
- Provided progress tracking & oversight
  - Goal achievement and management reporting

"DHS is honored and pleased to be working with SecureInfo Corporation in helping to meet the security needs of the Department."

Robert West
Chief Information Security Officer,
Department of Homeland Security

NASA – Case Study

Challenge

- Independent Validation & Verification of 300 NASA-wide systems
- Complete validations in 7-8 months
- Multiple Centers doing different process
- Not every system ready at the same time.

Solution

- Deployed multiple validation teams to 10 NASA centers using standardized process
- Sampling used to streamline "Like-systems"
- Grouping of systems = cost savings in Labor and travel
- Dramatic increase in complete packages to Authorizing Official

Value Proposition:

- ***Providing 25-35% cost savings through efficient execution***
- ***Assured quality of certification process***
- ***Uniquely mobilized to scale to customer demands***

Lessons Learned

1. Communication is key

- Partial understanding of C&A
- AO standards and expectations
    - Knee-jerk reactions
    - Negotiations

2. Mis-categorization of Security standards

- Involve Data Owners
- Fail Safe = High

3. Must have a C&A plan established

- Last ditch effort

Lessons Learned

4. Develop Baseline policy

- Standardized templates

5. Identify Common Controls

- Many systems can inherit controls

6. Train your personnel

- SP 800-37, Test & Evaluation
- Outsource services with qualified Experts with proven experience

7. Auditing

- Log Review
- System configurations

Lessons Learned

8. Choose proven Automated tools

- FISMA/C&A/Vulnerabilities
- Two heads are better than one

9. Stay on top of POA&M

- After accreditation decision POA&M not tracked
- Security issues not followed-up on

10. Define Annual Retesting of Security Controls

C&A Revitalization may be the answer !

Summary

- **C&A Challenge**
- **State of Affairs**
  - **10 Successful Steps**
- **Lessons Learned**
  - **10 Key Take-Aways**