Navigating the FISMA
Compliance Labyrinth

James D. Biggs, JD Biggs & Associates, Inc.
james@jdbiggs.com

Agu Ets, Project Performance Corporation
aets@PPC.com
<table>
<thead>
<tr>
<th>Agency</th>
<th>Grade</th>
<th>Agency</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Treasury</td>
<td>☢</td>
<td>State</td>
<td>☢</td>
</tr>
<tr>
<td>Agency for International Develop</td>
<td>☢</td>
<td>Defense</td>
<td>☢</td>
</tr>
<tr>
<td>Transportation</td>
<td>☢</td>
<td>SBA</td>
<td>☢</td>
</tr>
<tr>
<td>Nuclear Regulatory Commission</td>
<td>☢</td>
<td>NASA</td>
<td>☢</td>
</tr>
<tr>
<td>SSA</td>
<td>☢</td>
<td>Commerce</td>
<td>☢</td>
</tr>
<tr>
<td>EPA</td>
<td>☢</td>
<td>Veterans Affairs</td>
<td>☢</td>
</tr>
<tr>
<td>Labor</td>
<td>☢</td>
<td>Agriculture</td>
<td>☢</td>
</tr>
<tr>
<td>Justice</td>
<td>☢</td>
<td>HHS</td>
<td>☢</td>
</tr>
<tr>
<td>GSA</td>
<td>☢</td>
<td>Energy</td>
<td>☢</td>
</tr>
<tr>
<td>National Science Foundation</td>
<td>☢</td>
<td>HUD</td>
<td>☢</td>
</tr>
<tr>
<td>Education</td>
<td>☢</td>
<td>Homeland Security</td>
<td>☢</td>
</tr>
<tr>
<td>OPM</td>
<td>☢</td>
<td>Interior</td>
<td>☢</td>
</tr>
</tbody>
</table>
Challenges in Navigating the FISMA Compliance Labyrinth

- Understanding compliance requirements
- Ensuring policies in place and enforced
- Defining security requirements
- Managing effective risk assessments
- Performing certification and accreditation
- Interfacing with other processes
- Implementing automation to support compliance
How To Address These Challenges?
Government Directives
Driving Legislation

- E-Government Act of 2002 - Public Law 107-347
  - “To enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget.”

- Title III - Federal Information Security Management Act
  - “Provide for development and maintenance of minimum controls required to protect Federal information and information systems.”
  - Establish Agency Security Program
  - Establish annual reporting and assessment procedures

- Section 208 - Privacy Provisions
  - Ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.
  - Conduct Privacy Impact Assessment
Government Directives
Driving Legislation

- Office of Management and Budget (OMB) Circular A-130
- Appendix III - Security of Federal Automated Information Resources
- Supporting Memorandums
  - OMB Memorandum 03-19
  - OMB Memorandum 04-25
  - OMB Memorandum 05-15
Federal Information Security Management Act (FISMA) Methodology

**Version 4.1 - October 2005**

**Copyright 2003-2005 Agni R. Eun & James D. Biggs**

<table>
<thead>
<tr>
<th>Organizational Requirements (3544)</th>
<th>Provide protection commensurate with risk and magnitude of potential harm.</th>
<th>Provide security that supports operations and assets.</th>
<th>Delegate authority to CI for FISMA compliance.</th>
<th>Ensure sufficient trained personnel to support security requirements.</th>
<th>Ensure CIO reports annually on effectiveness of information security program.</th>
</tr>
</thead>
</table>

**Agency Program (3544)**

Develop, document and implement a security program to provide security for the information assets that support the operation of the agency.

<table>
<thead>
<tr>
<th>Security Policies and Procedures</th>
<th>Based on risk assessment results</th>
<th>Cost effective controls designed to reducing in-place &amp; planned risk.</th>
<th>Addressed throughout IT life-cycle</th>
<th>Compliant with FISMA Sec. 3544</th>
<th>Other applicable requirements</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Subordinate Systems Plans</th>
<th>Networks</th>
<th>IT systems</th>
<th>Groups of IT systems</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Continuity of Operations Plan</th>
<th>Plans and procedures in place</th>
<th>Mission critical systems</th>
<th>Support required operations</th>
<th>Protect assets</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Security Incident Reporting</th>
<th>Security incident procedure for detecting</th>
<th>Reporting</th>
<th>Mitigating damage risks</th>
<th>Notify Federal CIRF C</th>
<th>Consult with Law enforcement</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Testing and Evaluation Results</th>
<th>Performed at least annually</th>
<th>Management controls</th>
<th>Operational controls</th>
<th>Technical controls</th>
<th>All systems in inventory</th>
<th>Use independent evaluations</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Agency Risk Assessments</th>
<th>Identify threats</th>
<th>Identify vulnerabilities</th>
<th>Analyze security controls</th>
<th>Determine magnitude of harm</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Remedial Action Process</th>
<th>Remedial action process for failures</th>
<th>Implementing controls</th>
<th>Technical controls</th>
<th>Address deficiencies in policies</th>
<th>Procedures Practices</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Security Risk Management</th>
<th>Develop security life cycle</th>
<th>Define security policy</th>
<th>Define baseline common &amp; specific security requirements</th>
<th>Define baseline common &amp; system specific security controls</th>
<th>Define interconnection agreements</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Establish IT Environment</th>
<th>Continuity of operations plan</th>
<th>Define security policy</th>
<th>Define baseline common &amp; system specific security requirements</th>
<th>Define baseline common &amp; system specific security controls</th>
<th>Define interconnection agreements</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Guidance Documents</th>
<th>NIST SP 800-37</th>
<th>NIST SP 800-14</th>
<th>NIST SP 800-27</th>
<th>NIST SP 800-41</th>
<th>NIST SP 800-33</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Guidance Documents</th>
<th>NIST SP 800-35</th>
<th>NIST SP 800-36</th>
<th>NIST SP 800-40</th>
<th>NIST SP 800-45</th>
<th>NIST SP 800-53</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Establish IT Environment</th>
<th>Continuity of Support Plan</th>
<th>Continuity of System Operations Plan</th>
<th>Cyber Incident Response Plan</th>
<th>Disaster Recovery Plan</th>
<th>Incident Handling Plan</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Develop contingency planning policy statement</th>
<th>Develop security incident handling procedures</th>
<th>Develop contingency planning policy statement</th>
<th>Develop security incident handling procedures</th>
<th>Develop contingency planning policy statement</th>
<th>Develop security incident handling procedures</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Create Incident Response Plan</th>
<th>Develop incident response policy</th>
<th>Define response procedures</th>
<th>Develop US-CERT coordination</th>
<th>Develop an IT contingency plan</th>
<th>Plan testing, training, and exercises</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Test &amp; Evaluate Controls</th>
<th>Perform system security testing and evaluation</th>
<th>Perform SP 800-26 evaluation and audit</th>
<th>Evaluate CBA documentation</th>
<th>Update CBA documentation</th>
<th>STBE must include test cases, criteria, results using SP 800-53A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Remedy POA&amp;M Process</th>
<th>Identify weaknesses in systems</th>
<th>Define remedial action needed</th>
<th>Remedial costs as budget item</th>
<th>Fill out POA&amp;M matrix</th>
<th>Separate POA&amp;M for each system</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Remedial Action Process</th>
<th>Remedial action process for failures</th>
<th>Implementing controls</th>
<th>Technical controls</th>
<th>Address deficiencies in policies</th>
<th>Procedures Practices</th>
</tr>
</thead>
</table>

|-----------------------|-----------------------------|---------------------|-------------------------------|----------------------|---------------------|

|-----------------------------|--------------------------------------|------------------------|----------------------|

|---------------------|-------------------------|------------------------|--------------------------|-----------------------------|----------------------|

|---------------------|----------------------|--------------------------------------|----------------------|

<table>
<thead>
<tr>
<th>Documents Produced</th>
<th>Security Awareness &amp; Planning Training Plan</th>
<th>Awareness &amp; Training Metrics</th>
<th>Needs Assessment</th>
<th>Security Professional Development Syllabus</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Documents Produced</th>
<th>Security Test &amp; Evaluation Plan</th>
<th>System Self Assessment &amp; Audit</th>
<th>CBA Documentation Updates</th>
<th>Recommendations for Enhanced Security Controls</th>
</tr>
</thead>
</table>

|---------------------|-------------------------|----------------------|--------------------------|------------------|-------------------------------|

<table>
<thead>
<tr>
<th>Agency Reporting (3544)</th>
<th>The agency shall transmit a summary report of the annual IT security review including progress on correcting weaknesses and the results of the independent evaluation.</th>
<th>IAW OMB M-05-15</th>
<th>Tabular format - Tables A, B, C, D</th>
<th>+Agency FOIA</th>
<th>+Previous FOIA compliance report</th>
<th>+Previous CBA package</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Annual Independent Evaluation (3545)</th>
<th>The agency shall perform an annual independent evaluation to determine the effectiveness of the security program and practices at the agency.</th>
<th>Review security planning and the POA&amp;M for resolving security weaknesses</th>
<th>Review assigned security responsibilities and incident handling procedures</th>
<th>Review effectiveness of:</th>
<th>+Risk Assessments</th>
<th>+Capital Spending Security Training &amp; Awareness</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Create List of Conditions</th>
<th>Identify issues</th>
<th>Remedial &amp; Other issues</th>
<th>Update POA&amp;M</th>
</tr>
</thead>
</table>

| Incident Reporting (3544) | The agency shall have a documented procedure for reporting security incidents and sharing information regarding common vulnerabilities. | The agency shall have a documented procedure for coordinating with US CERT. | The agency shall have a documented procedure for patch management. | | | |
### FISMA Overview

| Organizational Requirements (3544) | • Delegate authority to CIO for FISMA compliance.  
• Provide protection commensurate with risk and magnitude of potential harm.  
• Provide security that supports operations and assets. | Ensure sufficient trained personnel to support security requirements  
• Ensure CIO reports annually on effectiveness of information security program. |

| Agency Program (3544 (b)) | Develop, document and implement a security program to provide security for the information assets that support the operation of the agency. |

| Agency Reporting (3544 (c)) | • The agency shall transmit a summary report annually of IT security reviews, progress & results of independent evaluations  
• Agency POA&M Previous IG report, FISMA compliance report  
Previous C&A package | IAW OMB M-05-15  
Tabular format - Tables A, B, C, & D |

| Annual Independent Evaluation (3545) | • Agency shall perform annual independent evaluations.  
• Review security planning and the POA&M for resolving security weaknesses.  
• Review assigned security responsibilities and incident handling procedures  
• Review effectiveness of Risk Assessments, IT Security Program, Capital Spending, & SETA |

| Incident Reporting (3546) | • The agency shall have a documented procedure for reporting security incidents and sharing information regarding common vulnerabilities. | • The agency shall have a documented procedure for coordinating with FedCIRC.  
• The agency shall have a documented procedure for patch management. |
FISMA
Agency Program (3544 (b))

- Security Policies and Procedures
  - Based on risk assessment results
  - Cost effective Controls
  - Addressed throughout lifecycle

- Guidance Documents (NIST -59, -60, -64; FIPS 199)

- Establish IT Environment
  - Classify IT systems
  - Define security policy
  - Define baseline common & system specific security controls

- Documents Produced
  - Systems Description Environment
  - System Security Policy
  - MOU, ISA documents
  - Supporting Policies
FISMA
Agency Program (3544 (b))

- Subordinate Systems Plans
  - Individual IT systems
  - Networks
  - Groups of IT systems

- Guidance Documents (NIST -18, -27; ISO/IEC 17799)

- Create Security Plan
  - Analysis with system owner
  - Determine management, operational and technical controls
  - Assemble security plan

- Documents Produced
  - Systems Description Environment
  - Boundary Definition
  - Rules of Behavior
  - Security Plan
FISMA
Agency Program (3544 (b))

- Continuity of Operations Plan
  - Identify mission critical systems
  - Put plans and procedures in place
  - Protect assets

- Guidance Documents (NIST -14, -34; ISO/IEC 17799)

- Perform Contingency Management Process
  - Develop contingency planning policy
  - Conduct business impact analysis
  - Develop recovery strategies and contingency plans

- Documents Produced
  - Continuity Plans (Business, Operations, Support)
  - Recovery Plans (Business, Disaster)
  - Incident Response Plan
Security Incident Reporting
- Install procedures for detecting, reporting and responding
- Mitigate damage
- Notify FedCIRC
- Consult with law enforcement, IG and others

Guidance Documents (NIST -14, -30, -61; ISO/IEC 17799)

Create Incident Response Plan
- Review incident response policy
- Define response procedures and FedCIRC coordination
- Interface with law enforcement

Documents Produced
- Incident Response Plan
- FedCIRC Coordination Plan
- Incident Logging Procedure
FISMA
Agency Program (3544 (b))

- **Training Plans**
  - Identify responsibility for compliance
  - Inform staff and contractors of security risks

- **Guidance Documents (NIST -14, -16, -50)**

- **Create Security Training Program**
  - Design awareness and training program
  - Develop instructional material for training program
  - Implement and evaluate awareness and training program

- **Documents Produced**
  - Security Awareness & Training Plan
  - Awareness & Training Metrics
  - Security Professional Development Syllabus
FISMA
Agency Program (3544 (b))

- Testing and Evaluation Results
  - Perform tests at least annually
  - Focus on management, operational and technical controls
  - Use independent evaluations

- Guidance Documents (NIST -26, -37, -42, -53A)

- Test and Evaluate Controls
  - Perform system testing and evaluation
  - Perform SP 800-26 Rev 1 evaluation and audit
  - Complete C&A security evaluation

- Documents Produced
  - Security Test & Evaluation Plan
  - System Self-Assessment and Audit
  - Recommendations for enhanced security controls
FISMA
Agency Program (3544 (b))

- **Agency Risk Assessments**
  - Identify threats and vulnerabilities
  - Analyze security controls
  - Determine magnitude of harm

- **Guidance Documents (NIST-14, -30, -64; ISO/IEC 17799)**

- **Perform Risk Assessments**
  - Define operational environment
  - Identify threats and vulnerabilities
  - Analyze security controls
  - Determine level of risk

- **Documents Produced**
  - Security Risk Assessment
  - System Security Policy
  - Management, Operational and Technical controls
  - Security Requirements
FISMA
Agency Program (3544 (b))

- Remedial Action Process
  - Define process for planning, implementing, evaluating and documenting remedial action
  - Address deficiencies in policy, procedures and practice
- Guidance Documents (OMB M-04-25, POA&M, NIST -55)
- Establish POA&M Process
  - Identify weaknesses in systems
  - Define remedial action needed
  - Budget costs of remedial action
  - Monitor progress of remedial action
- Documents Produced
  - Security Risk Assessment
  - System Security Policy
  - POA&M
FISMA also mandates compliance reporting to OMB

FISMA reporting receives very high visibility!

*Steps to “Get To Green” taken from a statement of the Honorable Karen Evans, Administrator for Electronic Government and IT, OMB, before the Committee on Government Reform, US House of Representatives, April 7, 2005*
Security Policies and Procedures

Where is my guiding light?
Policies Not Present or Enforced

- What are the problems?
  - Policies are not in place or are obsolete
  - Policy enforcement is lax
  - No process for reviewing and updating policies
  - Policies are ambiguous and loosely defined

- What may be the solution sets?
  - Establish policy taxonomy
  - Create policy review board and process
  - Assign a policy management team
### Security Policies and Procedures

<table>
<thead>
<tr>
<th>Management Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Planning Policy</td>
</tr>
<tr>
<td>Risk Assessment Policy</td>
</tr>
<tr>
<td>System and Services Acquisition Policy</td>
</tr>
<tr>
<td>Certification, Accreditation, and Security Assessments Policy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operational Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Awareness and Training Policy</td>
</tr>
<tr>
<td>Configuration Management Policy</td>
</tr>
<tr>
<td>Contingency Planning Policy</td>
</tr>
<tr>
<td>Media Protection Policy</td>
</tr>
<tr>
<td>Physical and Environmental Protection Policy</td>
</tr>
<tr>
<td>System and Information Integrity Policy</td>
</tr>
<tr>
<td>Incident Response Policy</td>
</tr>
<tr>
<td>System Maintenance Policy</td>
</tr>
<tr>
<td>Personnel Security Policy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technical Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control Policy</td>
</tr>
<tr>
<td>Auditing and Accountability Policy</td>
</tr>
<tr>
<td>Identification and Authentication Policy</td>
</tr>
<tr>
<td>System and Communications Protection Policy</td>
</tr>
</tbody>
</table>
RA-1: Risk Assessment Policy and Procedures

Policy 2.1 Risk Management

Description:
[Define Department/Division/Group] must complete security categorization and classification of information and conduct a comprehensive risk assessment on systems in accordance with the Risk Management standards and practices.
Policy 5.1 System Certification and Assessments

Description:
All [Define] systems must be certified and accredited by an officially designated accrediting authority (DAA) prior to operating in a production environment. [Define Department/Division/Group] must continuously monitor critical controls and establish and maintain Plan of Actions & Milestones (POA&M) in accordance with System Certification and Assessments standards and practices.
Security Requirements

What must I do to be secure??
Defining Requirements

- Baseline security requirements (BLSR) provide the foundation for the entire risk assessment process.
- BLSR are derived from Policies, Laws, Executive Orders, Directives, Regulations, Statutes
- Start with best practices (Don’t reinvent!)
- Project Management 101 – Establish Plan
  
  **Do Not Deviate**

- Define and formalize management, operational, and technical Policies
Defining Requirements and Controls

- Define & formalize Clear / Concise Requirements
  - Incremental Approach – 1st Management, 2nd Operational, 3rd Technical
  - (Remember TMI = Information Overload / Short Circuit)
  - Distribute for Review / Acceptance / Buy-in
  - Signature Authority – C-Level

- Mapping Exercise
  - Management Requirement
  - Operational Requirement
  - Technical Requirement
Creating a Value added RTM

Traditional Requirements Traceability Matrix (RTM)

<table>
<thead>
<tr>
<th>Req #</th>
<th>Requirement</th>
<th>Requirement Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>M-RA1</td>
<td>Perform security categorization in accordance with (IAW) FIPS – 199 and NIST Special Publications (SP) 800-59 &amp; 60. This is documented and approved by an appropriate senior official.</td>
<td>800-53: RA-1 Based on Agency Policy or Directive.</td>
</tr>
</tbody>
</table>

RTM is developed for Management, Operational, & Technical security requirements. Each requirement is written in sufficient detail & references a source for that requirement.
Managing Effective Risk Assessments

Are you sure we have looked at all risks?
Agency Risk Assessments

What are the problems?
- Rushed effort with inadequate planning
- Critical skills not in labor mix
- Coordinating access to facilities and systems
- Resource availability

What may be the solution sets?
- Include risk assessment in SDLC
- Project planning 101, 102 and 103
- Senior management involvement
## Vulnerability Identification

<table>
<thead>
<tr>
<th>Vulnerability Scanning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanning &amp; Enumeration</td>
</tr>
<tr>
<td>War Dialing</td>
</tr>
<tr>
<td>Wireless</td>
</tr>
<tr>
<td>Privilege Escalation and Back Door</td>
</tr>
<tr>
<td>Network Sniffers</td>
</tr>
<tr>
<td>File Integrity Checkers</td>
</tr>
<tr>
<td>Password Crackers</td>
</tr>
</tbody>
</table>

- **Vulnerability Assessment** – Network topology review; workstation & server security testing, 3rd party access review, regulation & policy compliance review, inbound/outbound traffic control, firewall & router ACLs to include log files, IDS setup & implementation and phone lines.

## Vulnerability Scanning Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Capabilities</th>
<th>Website</th>
<th>Linux</th>
<th>Win32</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>CyberCop Scanner is a network-based vulnerability-scanning tool that identifies security holes on network hosts.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISS Internet Scanner</td>
<td>Vulnerability scanner</td>
<td><a href="http://www.iss.net/">http://www.iss.net/</a></td>
<td>✗</td>
<td></td>
<td>$</td>
</tr>
<tr>
<td>Description</td>
<td>ISS Internet Scanner is a network-based vulnerability-scanning tool that identifies security holes on network hosts.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nessus</td>
<td>Vulnerability scanner</td>
<td>[<a href="http://www">http://www</a> nessus.org/](<a href="http://www">http://www</a> nessus.org/)</td>
<td>✗</td>
<td># (client only)</td>
<td>Free</td>
</tr>
<tr>
<td>Description</td>
<td>A freeware network-based vulnerability-scanning tool that identifies security holes on network hosts.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>SAINT is an updated and enhanced version of SATAN, is designed to assess the security of computer networks.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Sara is a freeware network-based vulnerability-scanning tool that identifies security holes on network hosts.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Certification and Accreditation

How can I manage all these tasks and documents?
Accreditation Decision

- I have determined that the risk to Agency Operations, Agency Assets, or Individuals resulting from the operation of the information system is acceptable.

- Accordingly, I am issuing an Authorization to Operate the information system in its existing operating environment.

- This security accreditation is my formal declaration that Adequate Security Controls have been implemented in the information system and that a satisfactory level of security is present in the system.
C&A Process Overview

- **C&A Process Phases**
  - Initiation Phase
  - Security Certification Phase
  - Security Accreditation Phase
  - Continuous Monitoring Phase

- **C&A Roles and Responsibilities**
  - Authorizing Official (AO)
  - Chief Information Officer (CIO)
  - Chief Information Security Officer (CISO)
  - Information System Owner (ISO)
  - Information System Security Officer (ISSO)
  - Certification Agent (CA)

### Security Certification Package
- Updated System Security Plan
- Completed Security Risk Assessment
- Updated Configuration Management Plan
- Contingency Management Plans
- Security Test & Evaluation Report
- User Manual W/SFUG
- Interconnection Security Agreements
- Memorandums of Agreement
- Completed Privacy Impact Assessment
- Federal Register System of Record Notice
- Plan of Action and Milestones (POAM)

### Security Accreditation Package
- Security Assessment Report
- Security Accreditation Decision Letter
- System Security Plan
- Plan of Action & Milestones (POAM)

### Certification & Accreditation (C&A) Package
C&A Process Tasks

- Required for major applications and general support systems
  - Evaluation of management, operational and technical security controls
  - Triggered by time (3 years) or significant changes
- Define accreditation boundaries, interfaces and subsystems and operating environment
- Assess risk for the environment within accreditation boundary
  - Threats and vulnerabilities
  - System test and evaluation
- Develop the Accreditation Package
  - Result of C&A activities by certifier.
  - Details all the activities from first three phases
- Make risk-based accreditation decision
  - Accept residual risk for that environment
  - Authorization to operate in that environment
Interface with Other Processes

Now how does this piece fit?
Contingency Planning

Types of Continuity and Contingency Documents

- **Continuity of Support Plan**
  - Focus on sustaining an organization’s business functions.
  - Applies to major or catastrophic events that close normal facility for an extended period.

- **Business Continuity Plan**
  - Focus on restoring an organization’s essential functions at an alternate site.

- **Disaster Recovery Plan**
  - Addresses the restoration of business processes after an emergency.
  - Protects against cyber attacks against an organization’s IT system(s).

- **Incident Response Plan**
  - Procedures for facility occupants during a threatening situation.

- **Occupant Emergency Plan**
  - Response procedures for facility occupants during a threatening situation.

- **Continuity of Operations Plan**
  - Focus on restoring an organization’s essential functions at an alternate site.

- **Business Recovery Plan**
  - Protects against cyber attacks against an organization’s IT system(s).

- **Contingency Planning**
Remedial Processes

- **POA&M**
  - Manage all known weaknesses in the POA&M
  - Verify and validate completed corrective actions

- **Maintain Security Requirements**
  - Maintain BLSR & BLPR under configuration control
  - Leverage existing and cost effective controls

- **Self Assessments**
  - Supports the C&A Continuous Monitoring process

- **OIG or GAO audits**
Using Automation Support for FISMA

How can I make this process fly?
Benefits of Automation Support

- Reduced Personnel Costs for Compliance
- Consistency in Assessments and Evaluations
- Documents Formatted Correctly
- System Inventory Management Automated
- Auditable Compliance Process
Criteria for Tool Selection

- Integration Potential with Existing Infrastructure
- User Interface Intuitive and Effective
- Capability for Audit Trail
- Output Formats for Documents and Reports
- Adaptability to Specific Agency Requirements
- Interface to POA&M Process
Sample of Vendor Products

- Automated Security Self-Assessment Tool (ASSET)
- Xacta Web C&A
- Xacta Commerce Trust
- Risk Management System (RMS)
- Risk Watch
- Trusted Agent FISMA
- Other Proprietary Support Tools
How everything fits together.
FISMA Compliance Avoids Red

Are you ready for an IG Inspection?
Had Enough?

Any Questions?
Navigating the FISMA Compliance Labyrinth

Thank You

James D. Biggs, 410-322-8245 james@jdbiggs.com

Agu Ets, 301-526-3327 aets@ppc.com
Project Performance Corporation http://www.ppc.com