Your Trusted Partner
for Improved
Security & Privacy

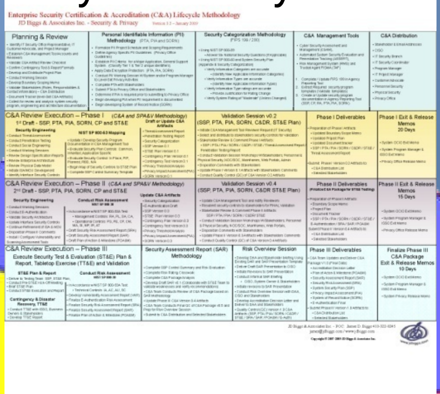
Strategies and Methodologies for Security & Privacy Professionals

FISSEA
22nd Annual Conference
March 24th 2009

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

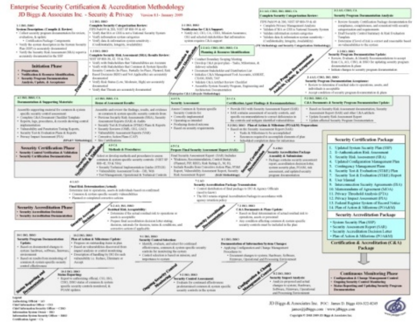
JDBIGGS
Associates
Security & Privacy Consulting

Enterprise Security C&A Lifecycle Methodology

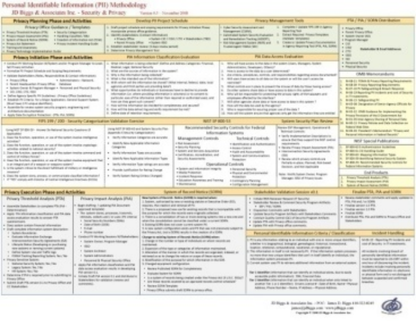

Enterprise Security Certification & Accreditation (C&A) Lifecycle Methodology
JD Biggs & Associates Inc. - Security & Privacy

Planning & Review
Personal Identifiable Information (PII) Methodology
Security Categorization Methodology
C&A Management Tools
C&A Distribution
C&A Review Execution – Phase I
Validation Session v0.2
Phase I Deliverables
Phase I Exit & Release Memos 20 Days
C&A Review Execution – Phase II
Validation Session v0.4
Phase II Deliverables
Phase II Exit & Release Memos 15 Days
C&A Review Execution – Phase III
Security Assessment Report (SAR) Methodology
Risk Overview Session
Phase III Deliverables
Finalize Phase III C&A Package Exit & Release Memos 10 Days

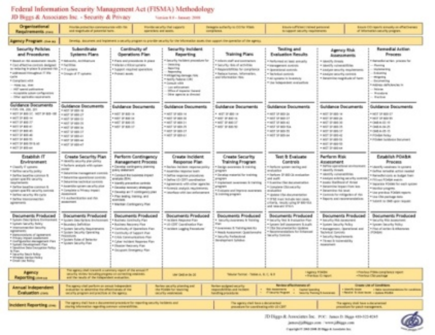
C&A Lifecycle Methodology


Enterprise Security Certification & Accreditation Methodology
JD Biggs & Associates Inc. - Security & Privacy

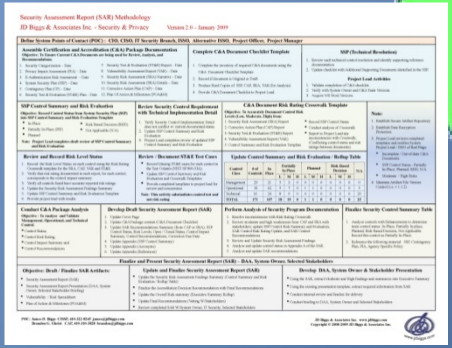
Personal Identifiable Information (PII) Methodology


Personal Identifiable Information (PII) Methodology
JD Biggs & Associates Inc. - Security & Privacy

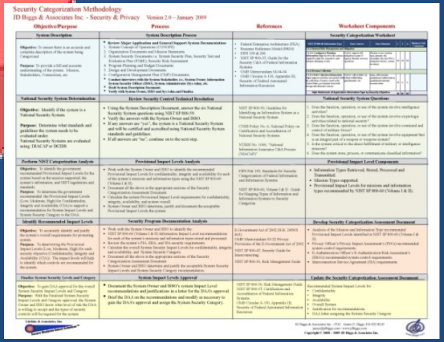
FISMA Methodology


Federal Information Security Management Act (FISMA) Methodology
JD Biggs & Associates Inc. - Security & Privacy

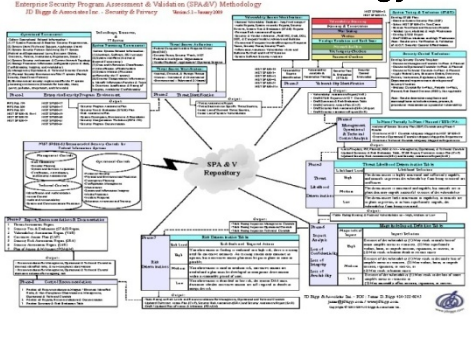
Security Assessment Report Methodology


Security Assessment Report (SAR) Methodology
JD Biggs & Associates Inc. - Security & Privacy

Security Categorization Methodology


Security Categorization Methodology
JD Biggs & Associates Inc. - Security & Privacy

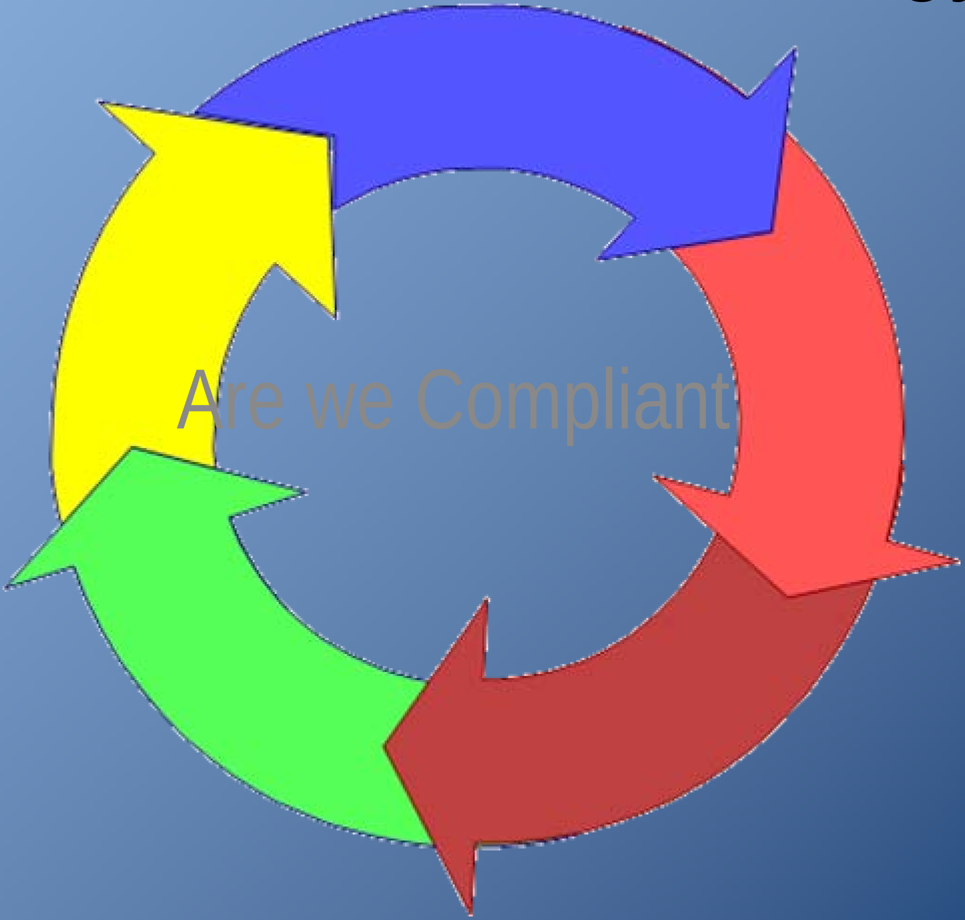
SPA&V Methodology

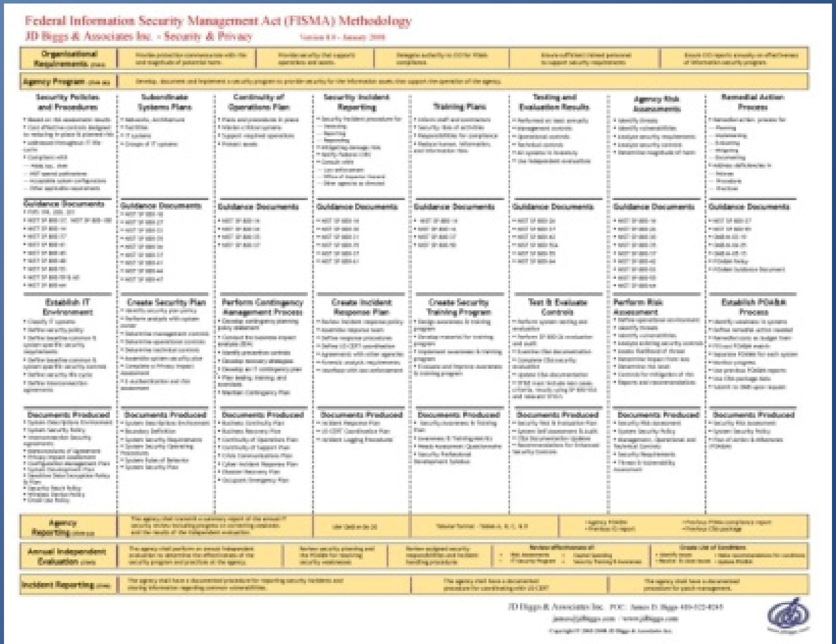

Enterprise Security Program Assessment & Validation (SPA&V) Methodology
JD Biggs & Associates Inc. - Security & Privacy
SPA & V Repository

Purpose of Strategies & Methodologies

- A graphical understanding of Federal Standards (NIST Special Publications, FIPS Publications, OMB Memorandums)
- Strategies in Developing Project Management Plans & Schedules
- Evaluate the Performance of Internal & Contractor Resources
- Roadmaps to Effectively Completing: Privacy Management, Security Categorization, Certification & Accreditation, Risk Assessment, Security Assessment Report
- Develop Enterprise Security Program and System Documentation
- Educate DAA, CIO, System Owners and Stakeholders
- Resolving Material Weaknesses and POA&M

FISMA Methodology





Federal Information Security Management Act (FISMA) Methodology

JD Biggs & Associates Inc. - Security & Privacy [illegible]

Organizational Requirements [illegible]	[illegible]		[illegible]		[illegible]	[illegible]	[illegible]
Agency Program [illegible]	[illegible]						
Security Policies and Procedures	Subordinate Systems Plans	Continuity of Operations Plan	Security Incident Reporting	Training Plans	Testing and Evaluation Results	Agency Risk Assessments	Remedial Action Process
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Guidance Documents	Guidance Documents	Guidance Documents	Guidance Documents	Guidance Documents	Guidance Documents	Guidance Documents	Guidance Documents
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Establish IT Environment	Create Security Plan	Perform Contingency Management Process	Create Incident Response Plan	Create Security Training Program	Test & Evaluate Controls	Perform Risk Assessment	Establish POA&M Process
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Documents Produced	Documents Produced	Documents Produced	Documents Produced	Documents Produced	Documents Produced	Documents Produced	Documents Produced
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Agency Reporting [illegible]	[illegible]		[illegible]	[illegible]		[illegible]	[illegible]
Annual Independent Evaluation [illegible]	[illegible]		[illegible]	[illegible]	[illegible]		[illegible]
Incident Reporting [illegible]	[illegible]			[illegible]		[illegible]	

JD Biggs & Associates Inc. [illegible]

[illegible]

FISMA Methodology

- This FISMA chart allows organizational stakeholders to examine System and Agency Program requirements and determine which areas need improvement.
- Five (5) Main Sections in the Legislation:
  - Organizational Requirements (3544)
  - Agency Program (3544 b)
  - Agency Reporting (3544 c)
  - Annual Independent Evaluation (3545)
  - Incident Reporting (3546)

Key Points of Agency Program

Agency Program (3544) (b)

1. Security Policies and Procedures
2. Subordinate Systems Plans
3. Continuity of Operations Plan
4. Security Incident Reporting
5. Training Plans
6. Testing and Evaluation Results
7. Agency Risk Assessments
8. Remedial Action Process

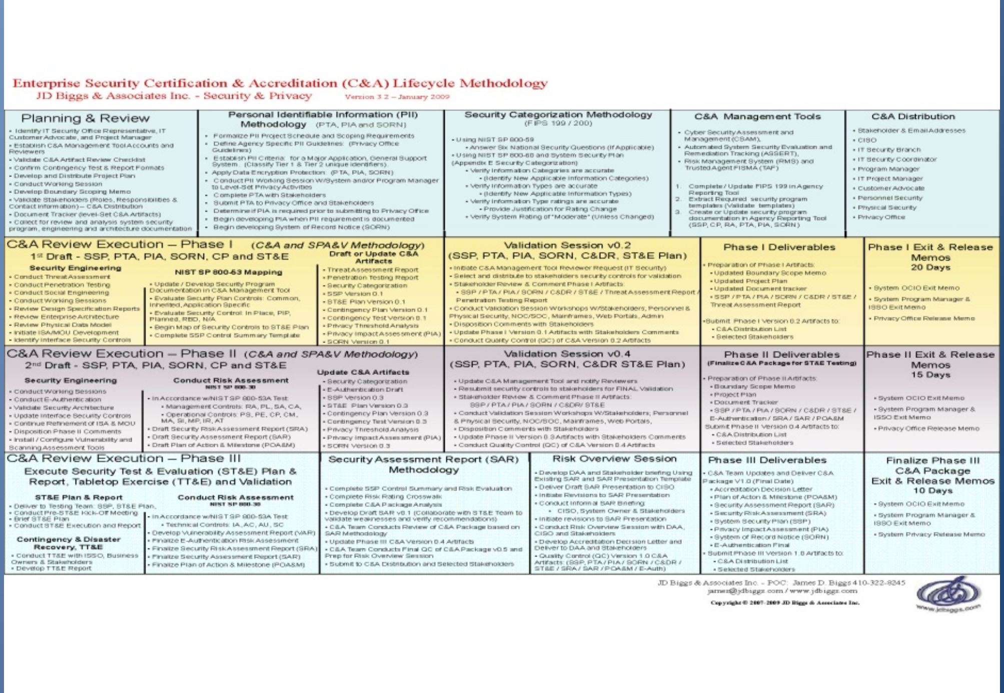
Strategies / Consideration

- Listed Requirements (Major Application / General Support System / Enterprise and Operating Units and Administrations)
- Guidance Documentation (Federal Standards)
- Project Planning Activities (High Level)
- Tangible Outputs (Documents Produced)

- Conduct Internal Assessments – Determine Completeness
- Apply Guidance Documentation – Produce / Test / Train
- Refine Guidance Documentation – C&A, Risk Management, Policies

Your Trusted Partner
for Improved
Security & Privacy

Enterprise Security Certification & Accreditation (C&A) Lifecycle Methodology



Enterprise Security Certification & Accreditation (C&A) Lifecycle Methodology

JD Biggs & Associates Inc. - Security & Privacy Version 3.2 – January 2009

Planning & Review

- Identify IT Security Office Representative, IT Customer Advocate, and Project Manager
- Establish C&A Management Tool Accounts and Reviewers
- Validate C&A Artifact Review Checklist
- Confirm Contingency Test & Report Formats
- Develop and Distribute Project Plan
- Conduct Working Session
- Develop Boundary Scoping Memo
- Validate Stakeholders (Roles, Responsibilities & Contact information) – C&A Distribution
- Document Tracker (level-Set C&A Artifacts)
- Collect for review and analysis system security program, engineering and architecture documentation

Personal Identifiable Information (PII) Methodology (PTA, PIA and SORN)

- Formalize PII Project Schedule and Scoping Requirements
- Define Agency Specific PII Guidelines: (Privacy Office Guidelines)
- Establish PII Criteria: for a Major Application, General Support System. (Classify Tier 1 & Tier 2 unique identifiers).
- Apply Data Encryption Protection: (PTA, PIA, SORN)
- Conduct PII Working Session W/System and/or Program Manager to Level-Set Privacy Activities
- Complete PTA with Stakeholders
- Submit PTA to Privacy Office and Stakeholders
- Determine if PIA is required prior to submitting to Privacy Office
- Begin developing PIA when PII requirement is documented
- Begin developing System of Record Notice (SORN)

Security Categorization Methodology (FIPS 199 / 200)

- Using NIST SP 800-59
  - Answer Six National Security Questions (If Applicable)
- Using NIST SP 800-60 and System Security Plan (Appendix E Security Categorization)
  - Verify Information Categories are accurate
    - (Identify New Applicable Information Categories)
  - Verify Information Types are accurate
    - (Identify New Applicable Information Types)
  - Verify Information Type ratings are accurate
    - Provide Justification for Rating Change
  - Verify System Rating of "Moderate" (Unless Changed)

C&A Management Tools

- Cyber Security Assessment and Management (CSAM),
- Automated System Security Evaluation and Remediation Tracking (ASSERT),
- Risk Management System (RMS) and Trusted Agent FISMA (TAF)

1. Complete / Update FIPS 199 in Agency Reporting Tool
2. Extract Required security program templates (Validate templates)
3. Create or Update security program documentation in Agency Reporting Tool (SSP, CP, RA, PTA, PIA, SORN)

C&A Distribution

- Stakeholder & Email Addresses
- CISO
- IT Security Branch
- IT Security Coordinator
- Program Manager
- IT Project Manager
- Customer Advocate
- Personnel Security
- Physical Security
- Privacy Office

C&A Review Execution – Phase I (*C&A and SPA&V Methodology*)

1st Draft - SSP, PTA, PIA, SORN, CP and ST&E

Security Engineering

- Conduct Threat Assessment
- Conduct Penetration Testing
- Conduct Social Engineering
- Conduct Working Sessions
- Review Design Specification Reports
- Review Enterprise Architecture
- Review Physical Data Model
- Initiate ISA/MOU Development
- Identify Interface Security Controls

NIST SP 800-53 Mapping

- Update / Develop Security Program Documentation in C&A Management Tool
- Evaluate Security Plan Controls: Common, Inherited, Application Specific
- Evaluate Security Control: In Place, PIP, Planned, RBD, N/A
- Begin Map of Security Controls to ST&E Plan
- Complete SSP Control Summary Template

Draft or Update C&A Artifacts

- Threat Assessment Report
- Penetration Testing Report
- Security Categorization
- SSP Version 0.1
- ST&E Plan Version 0.1
- Contingency Plan Version 0.1
- Contingency Test Version 0.1
- Privacy Threshold Analysis
- Privacy Impact Assessment (PIA)
- SORN Version 0.1

Validation Session v0.2 (SSP, PTA, PIA, SORN, C&DR, ST&E Plan)

- Initiate C&A Management Tool Reviewer Request (IT Security)
- Select and distribute to stakeholders security controls for validation
- Stakeholder Review & Comment Phase I Artifacts:
  - SSP / PTA / PIA / SORN / C&DR / ST&E / Threat Assessment Report / Penetration Testing Report
- Conduct Validation Session Workshops W/Stakeholders; Personnel & Physical Security, NOC/SOC, Mainframes, Web Portals, Admin
- Disposition Comments with Stakeholders
- Update Phase I Version 0.1 Artifacts with Stakeholders Comments
- Conduct Quality Control (QC) of C&A Version 0.2 Artifacts

Phase I Deliverables

- Preparation of Phase I Artifacts:
  - Updated Boundary Scope Memo
  - Updated Project Plan
  - Updated Document tracker
  - SSP / PTA / PIA / SORN / C&DR / ST&E / Threat Assessment Report
- Submit Phase I Version 0.2 Artifacts to:
  - C&A Distribution List
  - Selected Stakeholders

Phase I Exit & Release Memos 20 Days

- System OCIO Exit Memo
- System Program Manager & ISSO Exit Memo
- Privacy Office Release Memo

C&A Review Execution – Phase II (*C&A and SPA&V Methodology*)

2nd Draft - SSP, PTA, PIA, SORN, CP and ST&E

Security Engineering

- Conduct Working Sessions
- Conduct E-Authentication
- Validate Security Architecture
- Update Interface Security Controls
- Continue Refinement of ISA & MOU
- Disposition Phase II Comments
- Install / Configure Vulnerability and Scanning Assessment Tools

Conduct Risk Assessment
NIST SP 800-30

- In Accordance w/NIST SP 800-53A Test:
  - Management Controls: RA, PL, SA, CA,
  - Operational Controls: PS, PE, CP, CM, MA, SI, MP, IR, AT
- Draft Security Risk Assessment Report (SRA)
- Draft Security Assessment Report (SAR)
- Draft Plan of Action & Milestone (POA&M)

Update C&A Artifacts

- Security Categorization
- E-Authentication Draft
- SSP Version 0.3
- ST&E Plan Version 0.3
- Contingency Plan Version 0.3
- Contingency Test Version 0.3
- Privacy Threshold Analysis
- Privacy Impact Assessment (PIA)
- SORN Version 0.3

Validation Session v0.4 (SSP, PTA, PIA, SORN, C&DR ST&E Plan)

- Update C&A Management Tool and notify Reviewers
- Resubmit security controls to stakeholders for FINAL Validation
- Stakeholder Review & Comment Phase II Artifacts:
  SSP / PTA / PIA / SORN / C&DR/ ST&E
- Conduct Validation Session Workshops W/Stakeholders; Personnel & Physical Security, NOC/SOC, Mainframes, Web Portals,
- Disposition Comments with Stakeholders
- Update Phase II Version 0.3 Artifacts with Stakeholders Comments
- Conduct Quality Control (QC) of C&A Version 0.4 Artifacts

Phase II Deliverables

(Finalize C&A Package for ST&E Testing)

- Preparation of Phase II Artifacts:
  - Boundary Scope Memo
  - Project Plan
  - Document Tracker
  - SSP / PTA / PIA / SORN / C&DR / ST&E / E-Authentication / SRA / SAR / POA&M
- Submit Phase II Version 0.4 Artifacts to:
  - C&A Distribution List
  - Selected Stakeholders

Phase II Exit & Release Memos 15 Days

- System OCIO Exit Memo
- System Program Manager & ISSO Exit Memo
- Privacy Office Release Memo

C&A Review Execution – Phase III

Execute Security Test & Evaluation (ST&E) Plan & Report, Tabletop Exercise (TT&E) and Validation

ST&E Plan & Report

- Deliver to Testing Team: SSP, ST&E Plan,
- Conduct Pre-ST&E Kick-Off Meeting
- Brief ST&E Plan
- Conduct ST&E Execution and Report

Contingency & Disaster Recovery, TT&E

- Conduct TT&E with ISSO, Business Owners & Stakeholders
- Develop TT&E Report

Conduct Risk Assessment
NIST SP 800-30

- In Accordance w/NIST SP 800-53A Test:
  - Technical Controls: IA, AC, AU, SC
- Develop Vulnerability Assessment Report (VAR)
- Finalize E-Authentication Risk Assessment
- Finalize Security Risk Assessment Report (SRA)
- Finalize Security Assessment Report (SAR)
- Finalize Plan of Action & Milestone (POA&M)

Security Assessment Report (SAR) Methodology

- Complete SSP Control Summary and Risk Evaluation
- Complete Risk Rating Crosswalk
- Complete C&A Package Analysis
- Develop Draft SAR v0.1 (Collaborate with ST&E Team to validate weaknesses and verify recommendations)
- C&A Team Conducts Review of C&A Package based on SAR Methodology
- Update Phase III C&A Version 0.4 Artifacts
- C&A Team Conducts Final QC of C&A Package v0.5 and Prep for Risk Overview Session
- Submit to C&A Distribution and Selected Stakeholders

Risk Overview Session

- Develop DAA and Stakeholder briefing Using Existing SAR and SAR Presentation Template
- Deliver Draft SAR Presentation to CISO
- Initiate Revisions to SAR Presentation
- Conduct Informal SAR Briefing:
  - CISO, System Owner & Stakeholders
- Initiate revisions to SAR Presentation
- Conduct Risk Overview Session with DAA, CISO and Stakeholders
- Develop Accreditation Decision Letter and Deliver to DAA and Stakeholders
- Quality Control (QC) Version 1.0 C&A Artifacts: (SSP, PTA / PIA / SORN / C&DR / ST&E / SRA / SAR / POA&M / E-Auth)

Phase III Deliverables

- C&A Team Updates and Deliver C&A Package V1.0 (Final Date)
  - Accreditation Decision Letter
  - Plan of Action & Milestone (POA&M)
  - Security Assessment Report (SAR)
  - Security Risk Assessment (SRA)
  - System Security Plan (SSP)
  - Privacy Impact Assessment (PIA)
  - System of Record Notice (SORN)
  - E-Authentication Final
- Submit Phase III Version 1.0 Artifacts to:
  - C&A Distribution List
  - Selected Stakeholders

Finalize Phase III C&A Package Exit & Release Memos 10 Days

- System OCIO Exit Memo
- System Program Manager & ISSO Exit Memo
- System Privacy Release Memo

JD Biggs & Associates Inc. - POC: James D. Biggs 410-322-8245
james@jdbiggs.com / www.jdbiggs.com

www.jdbiggs.com

JDBIGGS
Associates
Security & Privacy Consulting

Purpose of C&A Lifecycle Methodology

- A structured approach to completing Certification or Recertification Activities for an Accreditation Decision (*Single or Multiple Systems*)
- Level-Set expectations of System Owner, Contractor and Stakeholders
- Control the Review of Security Artifacts and Testing of Management, Operational & Technical Controls
- Prevent the creation of phony security program documentation
- Applies other Methodologies to Complete:
  - Privacy Analysis / Management
  - Security Categorization
  - Risk Assessment / Reports / Overview Sessions

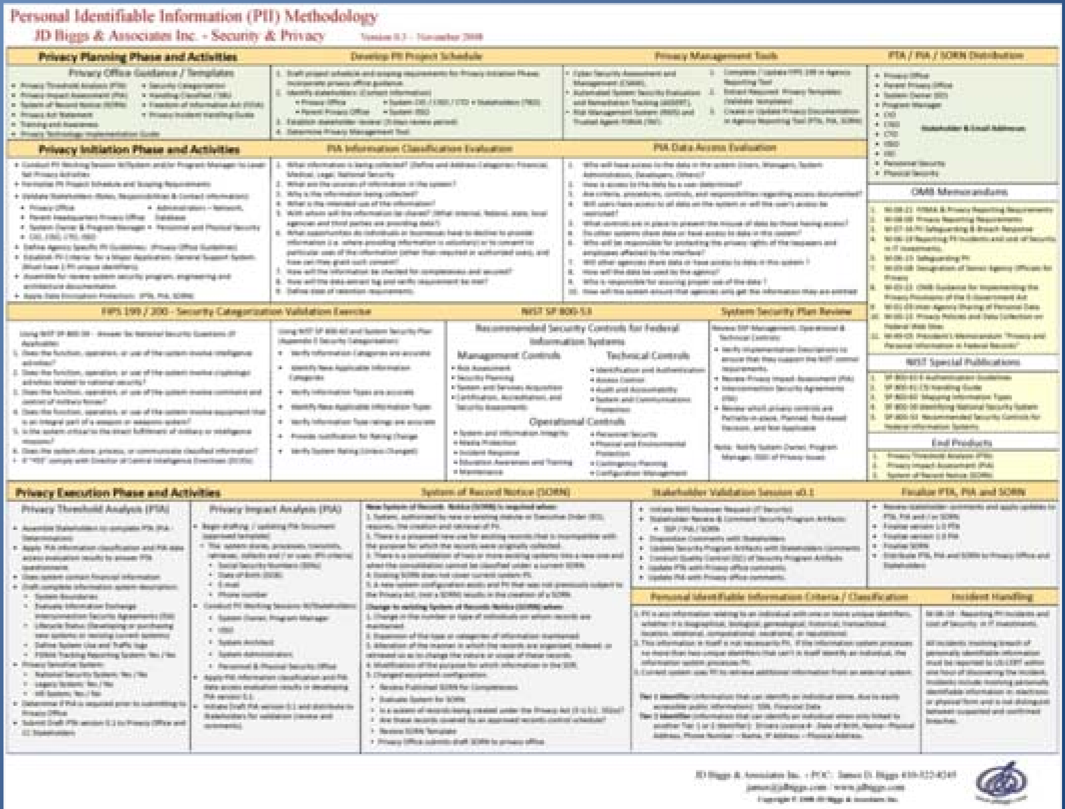
Planning and Review

- Establish Boundary Scoping Memo:
  - Identifies Critical Stakeholders e.g. DAA, IT Security Office, Privacy Coordinator, System Owner, Program Manager, Network & Security Operations
  - Define all required deliverables, reports, templates
  - Establish timelines for Privacy / Security Categorization / Control Testing….
  - Identify Stakeholders for Control Validation and Document Reviews
- Develop and Distribute Project Management Plan
- Establish C&A Management Tool Accounts
- Collect for Review and Analysis all System Security Program, Engineering, and Architecture Documentation

Your **T**rusted **P**artner
for **I**mproved
Security & **P**rivacy

Planning and Review

- Define Personal Identifiable Information (PII)
  - PTA, PIA, SORN
- Personal Identifiable Information Methodology
  - Draft SP 800-122



Personal Identifiable Information (PII) Methodology
JD Biggs & Associates Inc. - Security & Privacy

Privacy Planning Phase and Activities | Develop PII Project Schedule | Privacy Management Tools | PTA / PIA / SORN Distribution

Privacy Office Guidance / Templates

Privacy Initiation Phase and Activities | PIA Information Classification Evaluation | PIA Data Access Evaluation

OMB Memorandums

FIPS 199 / 200 - Security Categorization Validation Exercise | NIST SP 800-53 | System Security Plan Review

Recommended Security Controls for Federal Information Systems

Management Controls | Technical Controls | Operational Controls

NIST Special Publications

End Products

Privacy Execution Phase and Activities | System of Record Notice (SORN) | Stakeholder Validation Session v0.1 | Finalize PTA, PIA and SORN

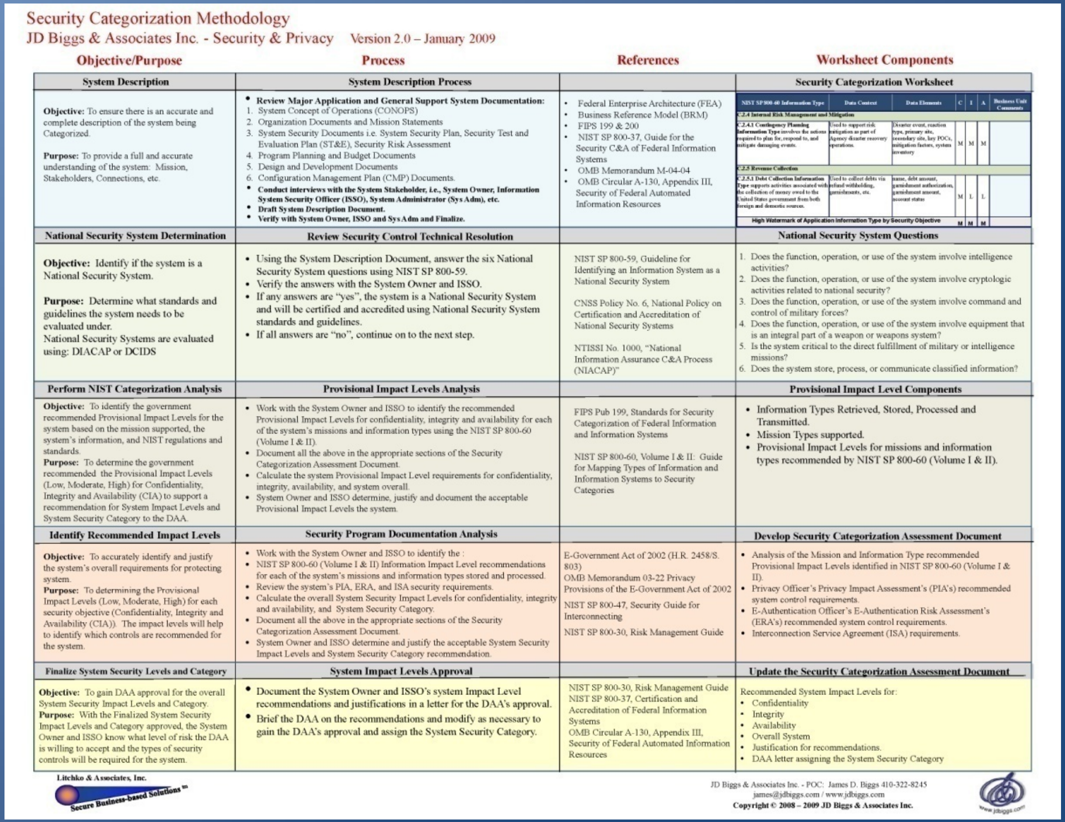
Privacy Threshold Analysis (PTA) | Privacy Impact Analysis (PIA)

Personal Identifiable Information Criteria / Classification | Incident Handling

JDBIGGS
Associates
Security & Privacy Consulting

Planning and Review

- Conduct Security Categorization
  - NIST SP 800-59
  - NIST SP 800-60
  - FIPS 199 - 200
- Security Categorization Methodology



Security Categorization Methodology

JD Biggs & Associates Inc. - Security & Privacy Version 2.0 – January 2009

<table>
<tr><th>Objective/Purpose</th><th>Process</th><th>References</th><th>Worksheet Components</th></tr>
<tr><td><b>System Description</b></td><td><b>System Description Process</b></td><td></td><td><b>Security Categorization Worksheet</b></td></tr>
<tr><td><b>Objective:</b> To ensure there is an accurate and complete description of the system being Categorized.
<b>Purpose:</b> To provide a full and accurate understanding of the system: Mission, Stakeholders, Connections, etc.</td><td>• <b>Review Major Application and General Support System Documentation:</b>
1. System Concept of Operations (CONOPS)
2. Organization Documents and Mission Statements
3. System Security Documents i.e. System Security Plan, Security Test and Evaluation Plan (ST&E), Security Risk Assessment
4. Program Planning and Budget Documents
5. Design and Development Documents
6. Configuration Management Plan (CMP) Documents.
• <b>Conduct interviews with the System Stakeholder, i.e., System Owner, Information System Security Officer (ISSO), System Administrator (Sys Adm), etc.</b>
• <b>Draft System Description Document.</b>
• <b>Verify with System Owner, ISSO and Sys Adm and Finalize.</b></td><td>• Federal Enterprise Architecture (FEA)
• Business Reference Model (BRM)
• FIPS 199 & 200
• NIST SP 800-37, Guide for the Security C&A of Federal Information Systems
• OMB Memorandum M-04-04
• OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources</td><td><table>
<tr><th>NIST SP 800-60 Information Type</th><th>Data Context</th><th>Data Elements</th><th>C</th><th>I</th><th>A</th><th>Business Unit Comments</th></tr>
<tr><td colspan="7"><b>C.2.4 Internal Risk Management and Mitigation</b></td></tr>
<tr><td><b>C.2.4.1 Contingency Planning Information Type</b> involves the actions required to plan for, respond to, and mitigate damaging events.</td><td>Used to support risk mitigation as part of Agency disaster recovery operations.</td><td>Disaster event, reaction type, primary site, secondary site, key POCs, mitigation factors, system inventory</td><td>M</td><td>M</td><td>M</td><td></td></tr>
<tr><td colspan="7"><b>C.2.5 Revenue Collection</b></td></tr>
<tr><td><b>C.2.5.1 Debt Collection Information Type</b> supports activities associated with the collection of money owed to the United States government from both foreign and domestic sources.</td><td>Used to collect debts via refund withholding, garnishments, etc.</td><td>name, debt amount, garnishment authorization, garnishment amount, account status</td><td>M</td><td>L</td><td>L</td><td></td></tr>
<tr><td colspan="3"><b>High Watermark of Application Information Type by Security Objective</b></td><td>M</td><td>M</td><td>M</td><td></td></tr>
</table></td></tr>
<tr><td><b>National Security System Determination</b></td><td><b>Review Security Control Technical Resolution</b></td><td></td><td><b>National Security System Questions</b></td></tr>
<tr><td><b>Objective:</b> Identify if the system is a National Security System.
<b>Purpose:</b> Determine what standards and guidelines the system needs to be evaluated under.
National Security Systems are evaluated using: DIACAP or DCIDS</td><td>• Using the System Description Document, answer the six National Security System questions using NIST SP 800-59.
• Verify the answers with the System Owner and ISSO.
• If any answers are "yes", the system is a National Security System and will be certified and accredited using National Security System standards and guidelines.
• If all answers are "no", continue on to the next step.</td><td>NIST SP 800-59, Guideline for Identifying an Information System as a National Security System
CNSS Policy No. 6, National Policy on Certification and Accreditation of National Security Systems
NTISSI No. 1000, "National Information Assurance C&A Process (NIACAP)"</td><td>1. Does the function, operation, or use of the system involve intelligence activities?
2. Does the function, operation, or use of the system involve cryptologic activities related to national security?
3. Does the function, operation, or use of the system involve command and control of military forces?
4. Does the function, operation, or use of the system involve equipment that is an integral part of a weapon or weapons system?
5. Is the system critical to the direct fulfillment of military or intelligence missions?
6. Does the system store, process, or communicate classified information?</td></tr>
<tr><td><b>Perform NIST Categorization Analysis</b></td><td><b>Provisional Impact Levels Analysis</b></td><td></td><td><b>Provisional Impact Level Components</b></td></tr>
<tr><td><b>Objective:</b> To identify the government recommended Provisional Impact Levels for the system based on the mission supported, the system's information, and NIST regulations and standards.
<b>Purpose:</b> To determine the government recommended the Provisional Impact Levels (Low, Moderate, High) for Confidentiality, Integrity and Availability (CIA) to support a recommendation for System Impact Levels and System Security Category to the DAA.</td><td>• Work with the System Owner and ISSO to identify the recommended Provisional Impact Levels for confidentiality, integrity and availability for each of the system's missions and information types using the NIST SP 800-60 (Volume I & II).
• Document all the above in the appropriate sections of the Security Categorization Assessment Document.
• Calculate the system Provisional Impact Level requirements for confidentiality, integrity, availability, and system overall.
• System Owner and ISSO determine, justify and document the acceptable Provisional Impact Levels the system.</td><td>FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems
NIST SP 800-60, Volume I & II: Guide for Mapping Types of Information and Information Systems to Security Categories</td><td>• Information Types Retrieved, Stored, Processed and Transmitted.
• Mission Types supported.
• Provisional Impact Levels for missions and information types recommended by NIST SP 800-60 (Volume I & II).</td></tr>
<tr><td><b>Identify Recommended Impact Levels</b></td><td><b>Security Program Documentation Analysis</b></td><td></td><td><b>Develop Security Categorization Assessment Document</b></td></tr>
<tr><td><b>Objective:</b> To accurately identify and justify the system's overall requirements for protecting system.
<b>Purpose:</b> To determining the Provisional Impact Levels (Low, Moderate, High) for each security objective (Confidentiality, Integrity and Availability (CIA)). The impact levels will help to identify which controls are recommended for the system.</td><td>• Work with the System Owner and ISSO to identify the :
• NIST SP 800-60 (Volume I & II) Information Impact Level recommendations for each of the system's missions and information types stored and processed.
• Review the system's PIA, ERA, and ISA security requirements.
• Calculate the overall System Security Impact Levels for confidentiality, integrity and availability, and System Security Category.
• Document all the above in the appropriate sections of the Security Categorization Assessment Document.
• System Owner and ISSO determine and justify the acceptable System Security Impact Levels and System Security Category recommendation.</td><td>E-Government Act of 2002 (H.R. 2458/S. 803)
OMB Memorandum 03-22 Privacy Provisions of the E-Government Act of 2002
NIST SP 800-47, Security Guide for Interconnecting
NIST SP 800-30, Risk Management Guide</td><td>• Analysis of the Mission and Information Type recommended Provisional Impact Levels identified in NIST SP 800-60 (Volume I & II).
• Privacy Officer's Privacy Impact Assessment's (PIA's) recommended system control requirements.
• E-Authentication Officer's E-Authentication Risk Assessment's (ERA's) recommended system control requirements.
• Interconnection Service Agreement (ISA) requirements.</td></tr>
<tr><td><b>Finalize System Security Levels and Category</b></td><td><b>System Impact Levels Approval</b></td><td></td><td><b>Update the Security Categorization Assessment Document</b></td></tr>
<tr><td><b>Objective:</b> To gain DAA approval for the overall System Security Impact Levels and Category.
<b>Purpose:</b> With the Finalized System Security Impact Levels and Category approved, the System Owner and ISSO know what level of risk the DAA is willing to accept and the types of security controls will be required for the system.</td><td>• Document the System Owner and ISSO's system Impact Level recommendations and justifications in a letter for the DAA's approval.
• Brief the DAA on the recommendations and modify as necessary to gain the DAA's approval and assign the System Security Category.</td><td>NIST SP 800-30, Risk Management Guide
NIST SP 800-37, Certification and Accreditation of Federal Information Systems
OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources</td><td>Recommended System Impact Levels for:
• Confidentiality
• Integrity
• Availability
• Overall System
• Justification for recommendations.
• DAA letter assigning the System Security Category</td></tr>
</table>

Litchko & Associates, Inc.
Secure Business-based Solutions ™

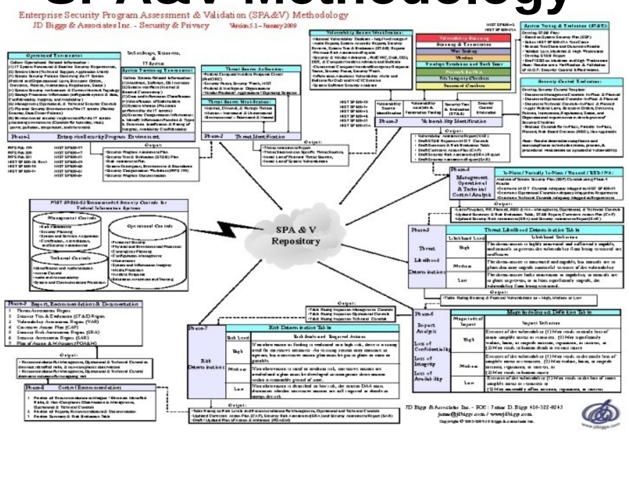
JD Biggs & Associates Inc. - POC: James D. Biggs 410-322-8245
james@jdbiggs.com / www.jdbiggs.com
Copyright © 2008 – 2009 JD Biggs & Associates Inc.

www.jdbiggs.com

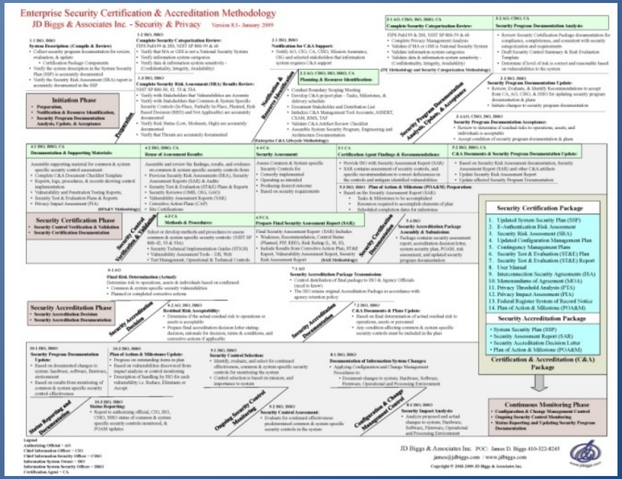
C&A Review Execution Phase I

- 1st Draft: SSP, PTA, PIA, SORN, CP, and ST&E

SPA&V Methodology


Enterprise Security Program Assessment & Validation (SPA&V) Methodology
JD Biggs & Associates Inc. - Security & Privacy
SPA & V Repository

C&A Methodology


Enterprise Security Certification & Accreditation Methodology
JD Biggs & Associates Inc. - Security & Privacy
Initiation Phase
Security Certification Phase
Security Accreditation Phase
Continuous Monitoring Phase
Security Certification Package
Security Accreditation Package
Certification & Accreditation (C&A) Package

Security Engineering: Threat Assessment, Penetration Testing, Social Engineering, Working Sessions.

Draft or Update C&A Artifacts: SSP, ST&E, PIA, PTA…

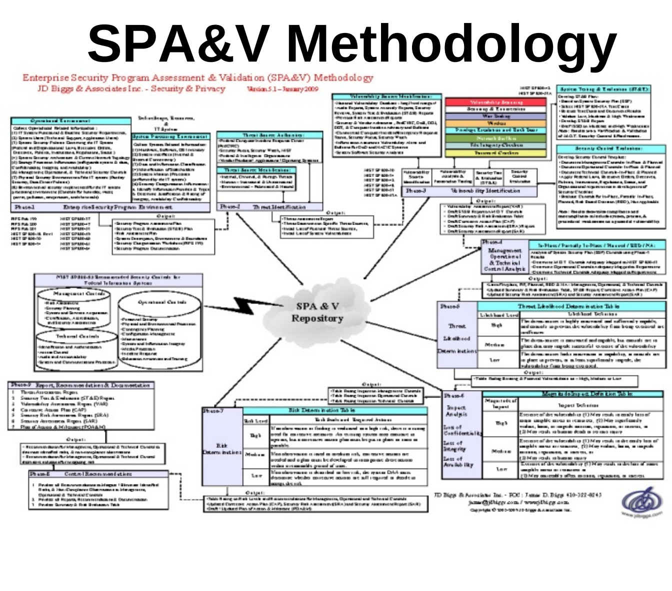
NIST SP 800-53 Mapping: Evaluate SSP Controls, Complete Control Summary.

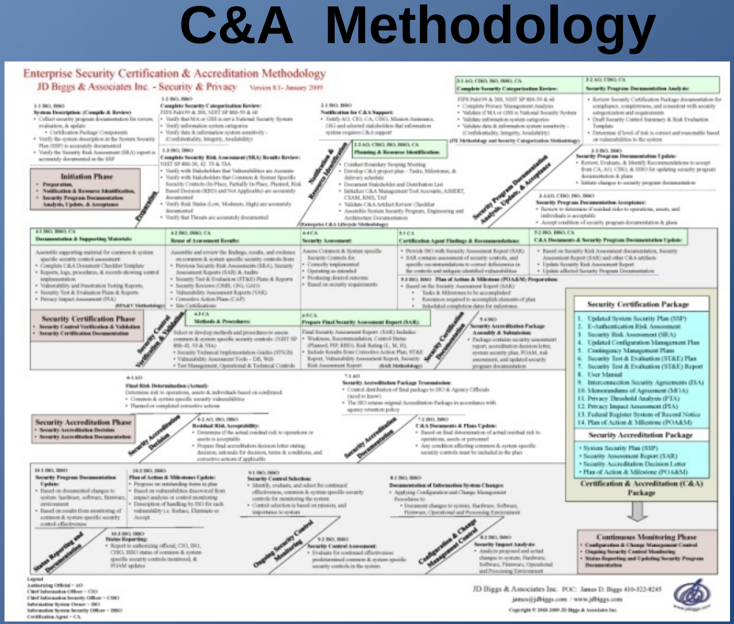
Validation Session v0.2: Select and Distribute Security Controls for Stakeholder Reviews .

Phase I Exit & Release Memos: OCIO, Program Manager, Privacy Office

C&A Review Execution Phase II

- 2nd Draft: SSP, PTA, PIA, SORN, CP, and ST&E


SPA&V Methodology
Enterprise Security Program Assessment & Validation (SPA&V) Methodology
JD Biggs & Associates Inc. - Security & Privacy
Version 5.1 – January 2009
SPA & V Repository


C&A Methodology
Enterprise Security Certification & Accreditation Methodology
JD Biggs & Associates Inc. - Security & Privacy
Version 8.1- January 2009
Initiation Phase
Security Certification Phase
Security Accreditation Phase
Security Certification Package
1. Updated System Security Plan (SSP)
2. E-Authentication Risk Assessment
3. Security Risk Assessment (SRA)
4. Updated Configuration Management Plan
5. Contingency Management Plans
6. Security Test & Evaluation (ST&E) Plan
7. Security Test & Evaluation (ST&E) Report
8. User Manual
9. Interconnection Security Agreements (ISA)
10. Memorandums of Agreement (MOA)
11. Privacy Threshold Analysis (PTA)
12. Privacy Impact Assessment (PIA)
13. Federal Register System of Record Notice
14. Plan of Action & Milestone (POA&M)
Security Accreditation Package
• System Security Plan (SSP)
• Security Assessment Report (SAR)
• Security Accreditation Decision Letter
• Plan of Action & Milestone (POA&M)
Certification & Accreditation (C&A) Package
Continuous Monitoring Phase
• Configuration & Change Management Control
• Ongoing Security Control Monitoring
• Status Reporting and Updating Security Program Documentation
JD Biggs & Associates Inc. POC: James D. Biggs 410-322-8245

- Continue Security Engineering and Updating C&A Artifacts
- Conduct Testing of Management & Operational Security Controls
- Begin Drafting Security Risk Assessment Report (SRA), Security Assessment Report (SAR), and Plan of Action & Milestone (POA&M)
- Conduct Validation Session v0.4

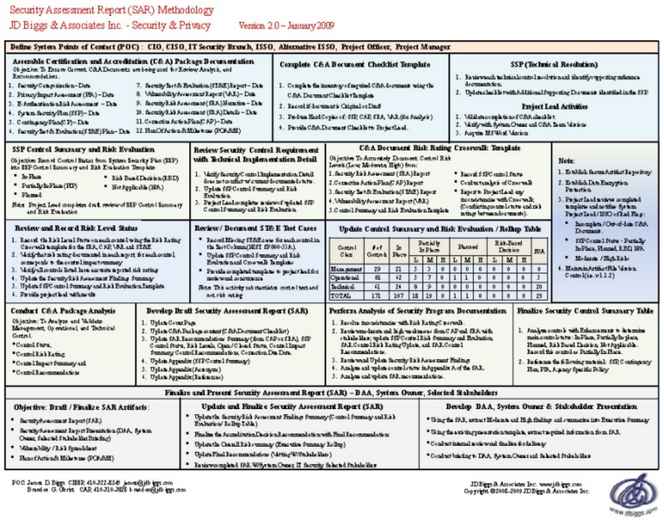
Phase II Exit & Release Memos: OCIO, Program Manager, Privacy Office

C&A Review Execution Phase III

- Execute ST&E Plan on Technical Controls, Tabletop Exercise (TT&E) and Risk Overview Session

- ST&E Plan & Report
- Contingency & Disaster Recovery, TT&E
- Conduct Risk Assessment (NIST SP 800-30 Technical Controls
- Finalize:
  - E-Authentication, SRA, SAR, POA&M

SAR Methodology



Security Assessment Report (SAR) Methodology
JD Biggs & Associates Inc. - Security & Privacy   Version 2.0 – January 2009

Define System Points of Contact (POC): CIO, CISO, IT Security Branch, ISSO, Alternative ISSO, Project Officer, Project Manager

Assemble Certification and Accreditation (C&A) Package Documentation

Objective: To Ensure Current C&A Documents are being used for Review Analysis, and Recommendations.

1. Security Categorization – Date
2. Privacy Impact Assessment (PIA) – Date
3. E-Authentication Risk Assessment – Date
4. System Security Plan (SSP) – Date
5. Contingency Plan (CP) – Date
6. Security Test & Evaluation (ST&E) Plan – Date
7. Security Test & Evaluation (ST&E) Report – Date
8. Vulnerability Assessment Report (VAR) – Date
9. Security Risk Assessment (SRA) Narrative – Date
10. Security Risk Assessment (SRA) Details – Date
11. Corrective Action Plan (CAP) – Date
12. Plan Of Action & Milestones (POA&M)

Complete C&A Document Checklist Template

1. Complete the inventory of required C&A documents using the C&A Document Checklist Template
2. Record if document is Original or Draft
3. Produce Hard Copies of: SSP, CAP, SRA, VAR (for Analysis)
4. Provide C&A Document Checklist to Project Lead.

SSP (Technical Resolution)

1. Review each technical control resolution and identify supporting reference documentation.
2. Update checklist with Additional Supporting Documents identified in the SSP.

Project Lead Activities

1. Validate completion of C&A checklist.
2. Verify with System Owner and C&A Team Versions
3. Acquire MS Word Version

SSP Control Summary and Risk Evaluation

Objective: Record Control Status from System Security Plan (SSP) into SSP Control Summary and Risk Evaluation Template

- In Place
- Partially In Place (PIP)
- Planned
- Risk Based Decision (RBD)
- Not Applicable (N/A)

Note: Project Lead completes draft review of SSP Control Summary and Risk Evaluation

Review Security Control Requirement with Technical Implementation Detail

1. Verify Security Control Implementation Detail does not conflict w/ current documented status.
2. Update SSP Control Summary and Risk Evaluation
3. Project Lead completes review of updated SSP Control Summary and Risk Evaluation.

C&A Document Risk Rating Crosswalk Template

Objective: To Accurately Document Control Risk Levels (Low, Moderate, High) from:

1. Security Risk Assessment (SRA) Report
2. Corrective Action Plan (CAP) Report
3. Security Test & Evaluation (ST&E) Report
4. Vulnerability Assessment Report (VAR)
5. Control Summary and Risk Evaluation Template

- Record SSP control Status
- Conduct analysis of Crosswalk
- Report to Project Lead any inconsistencies with Crosswalk; (Conflicting control status and risk ratings between documents).

Review and Record Risk Level Status

1. Record the Risk Level Status on each control using the Risk Rating Crosswalk template for the SRA, CAP, VAR and ST&E
2. Verify that risk rating documented in each report, for each control corresponds to the control impact summary
3. Verify all controls listed have accurate reported risk rating
4. Update the Security Risk Assessment Finding Summary
5. Update SSP Control Summary and Risk Evaluation Template
6. Provide project lead with results

Review / Document ST&E Test Cases

- Record Missing ST&E cases for each control in the Test Column (NIST SP 800-53A).
- Update SSP Control Summary and Risk Evaluation and Crosswalk Templates
- Provide completed templates to project lead for review and concurrence

Note: This activity substantiates control test and net risk rating

Update Control Summary and Risk Evaluation / Rollup Table

Control Class	# of Controls	In Place	Partially In Place			Planned			Risk-Based Decision			N/A
			L	M	H	L	M	H	L	M	H	
Management	29	21	5	3	0	0	0	0	0	0	0	0
Operational	81	62	5	7	0	1	1	0	0	0	0	5
Technical	61	24	8	9	0	0	0	0	0	0	0	20
TOTAL	171	107	18	19	0	1	1	0	0	0	0	25

Note:

1. Establish Secure Artifact Repository
2. Establish Data Encryption Protection
3. Project Lead reviews completed template and notifies System Project Lead / ISSO of Red Flag:
   - Incomplete / Out-of-date C&A Documents.
   - SSP Control Status - Partially In Place, Planned, RBD, N/A
   - Moderate / High Risks
4. Maintain Artifact File Version Control (i.e. v1.1.2)

Conduct C&A Package Analysis

Objective: To Analyze and Validate Management, Operational, and Technical Control.

- Control Status,
- Control Risk Rating
- Control Impact Summary and
- Control Recommendations

Develop Draft Security Assessment Report (SAR)

1. Update Cover Page
2. Update C&A Package content (C&A Document Checklist)
3. Update SAR Recommendations Summary (from CAP or SRA), SSP Control Status, Risk Levels, Open / Closed Status, Control Impact Summary, Control Recommendations, Correction Due Date.
4. Update Appendix (SSP Control Summary)
5. Update Appendix (Acronyms)
6. Update Appendix (References)

Perform Analysis of Security Program Documentation

1. Resolve inconsistencies with Risk Rating Crosswalk.
2. Review moderate and high weaknesses from CAP and SRA with stakeholders; update SSP Control Risk Summary and Evaluation, SAR Control Risk Rating Update, and SAR Control Recommendations.
3. Review and Update Security Risk Assessment Findings
4. Analyze and update control status in Appendix A of the SAR.
5. Analyze and update SAR recommendations.

Finalize Security Control Summary Table

1. Analyze controls with Enhancements to determine main control status: In Place, Partially In place, Planned, Risk Based Decision, Not Applicable. Record this control as Partially In Place.
2. Reference the following material: SSP, Contingency Plan, PIA, Agency Specific Policy

Finalize and Present Security Assessment Report (SAR) – DAA, System Owner, Selected Stakeholders

Objective: Draft / Finalize SAR Artifacts:

- Security Assessment Report (SAR)
- Security Assessment Report Presentation (DAA, System Owner, Selected Stakeholder Briefing)
- Vulnerability / Risk Spreadsheet
- Plan of Action & Milestones (POA&M)

Update and Finalize Security Assessment Report (SAR)

- Update the Security Risk Assessment Findings Summary (Control Summary and Risk Evaluation / Rollup Table)
- Finalize the Accreditation Decision Recommendation with Final Recommendations
- Update the Overall Risk summary (Executive Summary Rollup)
- Update Final Recommendations (Vetting W/ Stakeholders)
- Review completed SAR W/ System Owner, IT Security, Selected Stakeholders

Develop DAA, System Owner & Stakeholder Presentation

- Using the SAR, extract Moderate and High findings and summarize into Executive Summary
- Using the existing presentation template, extract required information from SAR.
- Conduct internal review and finalize for delivery
- Conduct briefing to DAA, System Owner and Selected Stakeholders

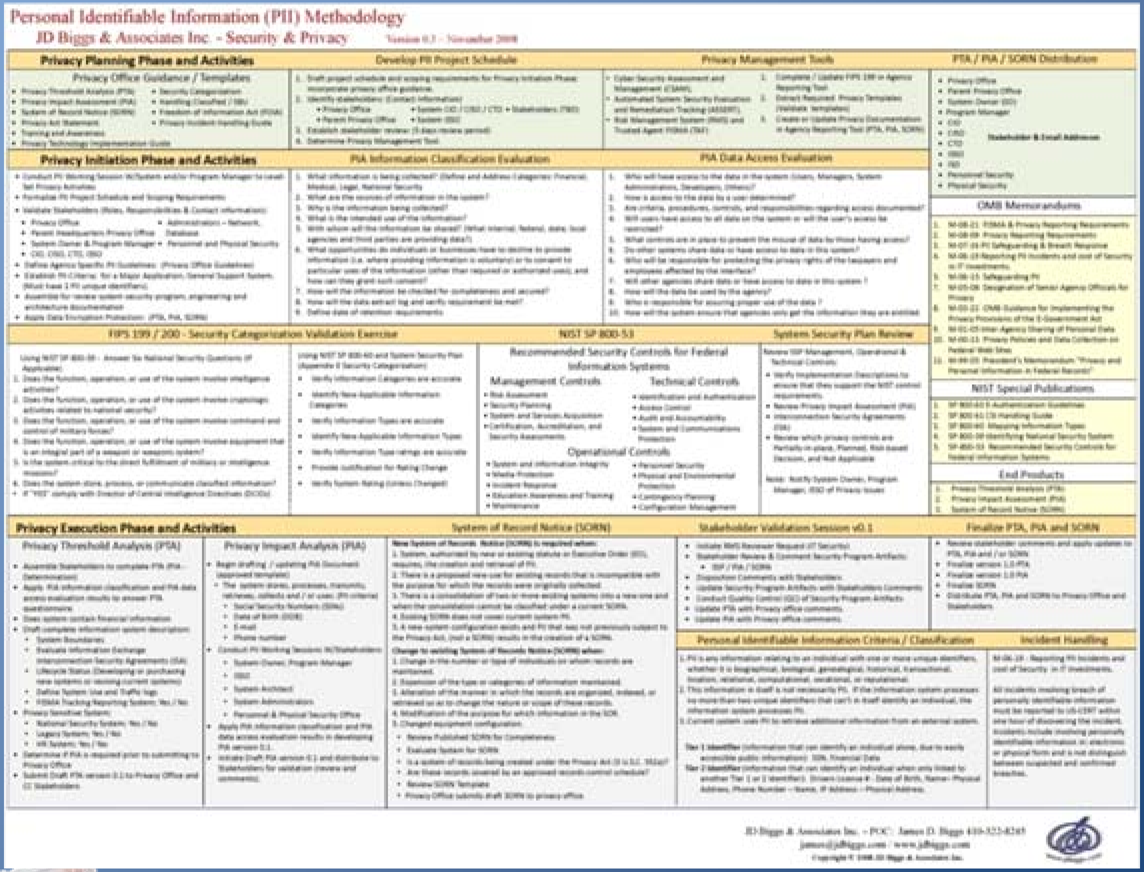
POC: James D. Biggs CISSP, 410-322-8246 james@jdbiggs.com
Brandon G. Christ CAP, 410-310-3828 brandon@jdbiggs.com

JD Biggs & Associates Inc. www.jdbiggs.com
Copyright ©2008-2009 JD Biggs & Associates Inc.

Complete: SSP Control Summary, Risk Evaluation, Risk Rating Crosswalk, C&A Package Analysis

Finalize Phase III Exit & Release Memos: OCIO, Program Manager, Privacy Office

Privacy Methodology



Personal Identifiable Information (PII) Methodology

JD Biggs & Associates Inc. - Security & Privacy   Version 0.3 - November 2008

Privacy Planning Phase and Activities

Privacy Office Guidance / Templates

- Privacy Threshold Analysis (PTA)
- Privacy Impact Assessment (PIA)
- System of Record Notice (SORN)
- Privacy Act Statement
- Training and Awareness
- Privacy Technology Implementation Guide
- Security Categorization
- Handling Classified / SBU
- Freedom of Information Act (FOIA)
- Privacy Incident Handling Guide

Develop PII Project Schedule

1. Draft project schedule and scoping requirements for Privacy Initiation Phase incorporate privacy office guidance.
2. Identify stakeholders (Contact information)
   - Privacy Office
   - Parent Privacy Office
   - System CIO / CISO / CTO
   - System ISSO
   - Stakeholders (TBD)
3. Establish stakeholder review (5 days review period)
4. Determine Privacy Management Tool

Privacy Management Tools

- Cyber Security Assessment and Management (CSAM)
- Automated System Security Evaluation and Remediation Tracking (ASSERT)
- Risk Management System (RMS) and Trusted Agent FISMA (TAF)

1. Complete / Update FIPS 199 in Agency Reporting Tool
2. Extract Required Privacy Templates (Validate templates)
3. Create or Update Privacy Documentation in Agency Reporting Tool (PTA, PIA, SORN)

PTA / PIA / SORN Distribution

- Privacy Office
- Parent Privacy Office
- System Owner (SO)
- Program Manager
- CIO
- CISO
- CTO
- ISSO
- ISO
- Personnel Security
- Physical Security

Stakeholder & Email Addresses

Privacy Initiation Phase and Activities

- Conduct PII Working Session W/System and/or Program Manager to Level Set Privacy Activities
- Formalize PII Project Schedule and Scoping Requirements
- Validate Stakeholders (Roles, Responsibilities & Contact information)
  - Privacy Office
  - Parent Headquarters Privacy Office
  - System Owner & Program Manager
  - CIO, CISO, CTO, ISSO
  - Administrators – Network, Database
  - Personnel and Physical Security
- Define Agency Specific PII Guidelines: (Privacy Office Guidelines)
- Establish PII Criteria: for a Major Application, General Support System. (Must have 2 PII unique identifiers)
- Assemble for review system security program, engineering and architecture documentation
- Apply Data Encryption Protection: (PTA, PIA, SORN)

PIA Information Classification Evaluation

1. What information is being collected? (Define and Address Categories: Financial, Medical, Legal, National Security
2. What are the sources of information in the system?
3. Why is the information being collected?
4. What is the intended use of the information?
5. With whom will the information be shared? (What internal, federal, state, local agencies and third parties are providing data?)
6. What opportunities do individuals or businesses have to decline to provide information (i.e. where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can they grant such consent?
7. How will the information be checked for completeness and accuracy?
8. How will the data extract log and verify requirement be met?
9. Define date of retention requirements.

PIA Data Access Evaluation

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
2. How is access to the data by a user determined?
3. Are criteria, procedures, controls, and responsibilities regarding access documented?
4. Will users have access to all data on the system or will the user's access be restricted?
5. What controls are in place to prevent the misuse of data by those having access?
6. Do other systems share data or have access to data in this system?
6. Who will be responsible for protecting the privacy rights of the taxpayers and employees affected by the interface?
7. Will other agencies share data or have access to data in this system ?
8. How will the data be used by the agency?
9. Who is responsible for assuring proper use of the data ?
10. How will the system ensure that agencies only get the information they are entitled

OMB Memorandums

1. M-08-21 FISMA & Privacy Reporting Requirements
2. M-08-09 Privacy Reporting Requirements
3. M-07-16 PII Safeguarding & Breach Response
4. M-06-19 Reporting PII Incidents and cost of Security in IT Investments
5. M-06-15 Safeguarding PII
7. M-05-08 Designation of Senior Agency Officials for Privacy
8. M-03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act
9. M-01-05 Inter Agency Sharing of Personal Data
10. M-00-13 Privacy Policies and Data Collection on Federal Web Sites
11. M-99-05 President's Memorandum "Privacy and Personal Information in Federal Records"

FIPS 199 / 200 - Security Categorization Validation Exercise

Using NIST SP 800-59 - Answer Six National Security Questions (If Applicable)

1. Does the function, operation, or use of the system involve intelligence activities?
2. Does the function, operation, or use of the system involve cryptologic activities related to national security?
3. Does the function, operation, or use of the system involve command and control of military forces?
4. Does the function, operation, or use of the system involve equipment that is an integral part of a weapon or weapons system?
5. Is the system critical to the direct fulfillment of military or intelligence missions?
6. Does the system store, process, or communicate classified information?

- If "YES" comply with Director of Central Intelligence Directives (DCIDs)

Using NIST SP 800-60 and System Security Plan (Appendix E Security Categorization)

- Verify Information Categories are accurate
- Identify New Applicable Information Categories
- Verify Information Types are accurate
- Identify New Applicable Information Types
- Verify Information Type ratings are accurate
- Provide Justification for Rating Change
- Verify System Rating (Unless Changed)

NIST SP 800-53

Recommended Security Controls for Federal Information Systems

Management Controls

- Risk Assessment
- Security Planning
- System and Services Acquisition
- Certification, Accreditation, and Security Assessments

Technical Controls

- Identification and Authentication
- Access Control
- Audit and Accountability
- System and Communications Protection

Operational Controls

- System and Information Integrity
- Media Protection
- Incident Response
- Education Awareness and Training
- Maintenance
- Personnel Security
- Physical and Environmental Protection
- Contingency Planning
- Configuration Management

System Security Plan Review

Review SSP Management, Operational & Technical Controls

- Verify Implementation Descriptions to ensure that they support the NIST control requirements.
- Review Privacy Impact Assessment (PIA)
- Interconnection Security Agreements (ISA)
- Review which privacy controls are Partially in place, Planned, Risk based Decision, and Not Applicable

Note: Notify System Owner, Program Manager, ISSO of Privacy Issues

NIST Special Publications

1. SP 800-63 E-Authentication Guidelines
2. SP 800-61 CSI Handling Guide
3. SP 800-60 Mapping Information Types
4. SP 800-59 Identifying National Security System
5. SP 800-53 Recommended Security Controls for Federal Information Systems

End Products

1. Privacy Threshold Analysis (PTA)
2. Privacy Impact Assessment (PIA)
3. System of Record Notice (SORN)

Privacy Execution Phase and Activities

Privacy Threshold Analysis (PTA)

- Assemble Stakeholders to complete PTA (PIA Determination)
- Apply PIA information classification and PIA data access evaluation results to answer PTA questionnaire
- Does system contain financial information
- Draft complete information system description
  - System Boundaries
  - Evaluate Information Exchange Interconnection Security Agreements (ISA)
  - Lifecycle Status (Developing or purchasing new systems or revising current systems)
  - Define System Use and Traffic logs
  - FISMA Tracking Reporting System: Yes / No
- Privacy Sensitive System
  - National Security System: Yes / No
  - Legacy System: Yes / No
  - HR System: Yes / No
- Determine if PIA is required prior to submitting to Privacy Office
- Submit Draft PTA version 0.1 to Privacy Office and CC Stakeholders

Privacy Impact Analysis (PIA)

- Begin drafting / updating PIA Document (approved template)
  - The system stores, processes, transmits, retrieves, collects and / or uses (PII criteria)
    - Social Security Numbers (SSN)
    - Date of Birth (DOB)
    - E-mail
    - Phone number
- Conduct PII Working Sessions W/Stakeholders
  - System Owner, Program Manager
  - ISSO
  - System Architect
  - System Administrators
  - Personnel & Physical Security Office
- Apply PIA information classification and PIA data access evaluation results in developing PIA version 0.1
- Initiate Draft PIA version 0.1 and distribute to Stakeholders for validation (review and comments)

System of Record Notice (SORN)

New System of Records Notice (SORN) is required when:

1. System, authorized by new or existing statute or Executive Order (EO), requires the creation and retrieval of PII.
2. There is a proposed new use for existing records that is incompatible with the purpose for which the records were originally collected.
3. There is a consolidation of two or more existing systems into a new one and when the consolidation cannot be classified under a current SORN.
4. Existing SORN does not cover current system PII.
5. A new system configuration exists and PII that was not previously subject to the Privacy Act, (not a SORN) results in the creation of a SORN.

Change to existing System of Records Notice (SORN) when:

1. Change in the number or type of individuals on whom records are maintained.
2. Expansion of the type or categories of information maintained.
3. Alteration of the manner in which the records are organized, indexed, or retrieved so as to change the nature or scope of these records.
4. Modification of the purpose for which information in the SOR
5. Changed equipment configuration.

- Review Published SORN for Completeness
- Evaluate System for SORN
- Is a system of records being created under the Privacy Act (5 U.S.C. 552a)?
- Are these records covered by an approved records control schedule?
- Review SORN Template
- Privacy Office submits draft SORN to privacy office.

Stakeholder Validation Session v0.1

- Initiate RMS Reviewer Request (IT Security)
- Stakeholder Review & Comment Security Program Artifacts
  - SSP / PIA / SORN
- Disposition Comments with Stakeholders
- Update Security Program Artifacts with Stakeholders Comments
- Conduct Quality Control (QC) of Security Program Artifacts
- Update PTA with Privacy office comments
- Update PIA with Privacy office comments

Finalize PTA, PIA and SORN

- Review stakeholder comments and apply updates to PTA, PIA and / or SORN
- Finalize version 1.0 PTA
- Finalize version 1.0 PIA
- Finalize SORN
- Distribute PTA, PIA and SORN to Privacy Office and Stakeholders

Personal Identifiable Information Criteria / Classification

1. PII is any information relating to an individual with one or more unique identifiers, whether it is biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational, or reputational.
2. This information in itself is not necessarily PII. If the information system processes no more than two unique identifiers that can't in itself identify an individual, the information system processes PII.
3. Current system uses PII to retrieve additional information from an external system.

Tier 1 Identifier (Information that can identify an individual alone, due to easily accessible public information): SSN, Financial Data

Tier 2 Identifier (Information that can identify an individual when only linked to another Tier 1 or 2 Identifier): Drivers License #, Date of Birth, Name- Physical Address, Phone Number – Name, IP Address – Physical Address

Incident Handling

M-06-19 - Reporting PII Incidents and cost of Security in IT Investments.

All incidents involving breach of personally identifiable information must be reported to US-CERT within one hour of discovering the incident. Incidents include involving personally identifiable information in electronic or physical form and is not distinguish between suspected and confirmed breaches.

JD Biggs & Associates Inc. – POC: James D. Biggs [illegible]
james@jdbiggs.com / www.jdbiggs.com
Copyright © 2008 JD Biggs & Associates Inc.

Protecting Personal Identifiable Information (PII)

PII Methodology

- These 3 phases apply to systems in Development, Production or affected by Significant Change.
- This chart outlines a proven strategy for creating required Privacy Documentation and Validating the contents with agency stakeholders.
- Incorporates Federal Standards – OMB Memorandums / NIST Pubs
- Stakeholder Involvement during Planning / Initiation / Execution
- Establishes PII Criteria and Classification, Information Classification and Data Access Evaluations Questions

PII Policy OMB

- M-08-21 & M-07-19, FISMA & Privacy Reporting Requirements
- M-08-09 Privacy Reporting Requirements
- M-07-16 PII Safeguarding & Breach Response
- M-06-19 Reporting PII Incidents and cost of Security in IT Investments.
- M-06-15 Safeguarding PII
- M-05-08 Designation of Senior Agency Officials for Privacy
- M-03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act
- M-01-05 Inter-Agency Sharing of Personal Data
- M-00-13 Privacy Policies and Data Collection on Federal Web Sites
- M-99-05 President's Memorandum "Privacy and Personal Information in Federal Records"

OMB M-07-16

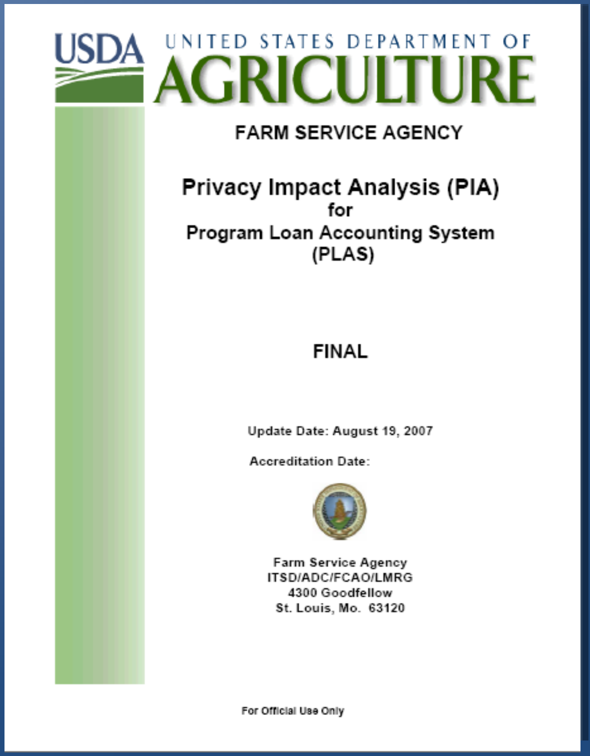
What is Personally Identifiable Information?

OMB M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information

- The term “Personally Identifiable Information (PII)” refers to information which can be used to distinguish or trace an individual's identity, such as their Name, Social Security Number, Biometric Records, etc. alone (Tier 1), or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc (Tier 2).

Privacy Office Guidance / Templates

- Privacy Threshold Analysis (PTA)
- Privacy Impact Assessment (PIA)
- System of Record Notice (SORN)
- Privacy Act Statement
- Training and Awareness
- Security Categorization
- Handling Classified / SBU
- Freedom of Information Act (FOIA)
- Privacy Incident Handling Guide



USDA UNITED STATES DEPARTMENT OF AGRICULTURE

FARM SERVICE AGENCY

Privacy Impact Analysis (PIA)
for
Program Loan Accounting System
(PLAS)

FINAL

Update Date: August 19, 2007

Accreditation Date:

Farm Service Agency
ITSD/ADC/FCAO/LMRG
4300 Goodfellow
St. Louis, Mo. 63120

For Official Use Only

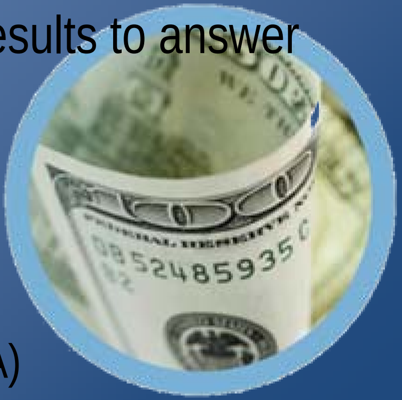
PIA Information Classification Evaluation

1. What information is being collected? (Define and Address Categories: Financial, Medical, Legal, National Security)
2. What are the sources of information in the system?
3. Why is the information being collected?
4. What is the intended use of the information?
5. With whom will the information be shared? (What internal, federal, state, local agencies and third parties are providing data?)
6. What opportunities do individuals or businesses have to decline to provide information (i.e. where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can they grant such consent?
7. How will the information be checked for completeness and secured?
8. How will the data extract log and verify requirement be met?
9. Define date of retention requirements.

PIA Data Access Evaluation

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
2. How is access to the data by a user determined?
3. Are criteria, procedures, controls, and responsibilities regarding access documented?
4. Will users have access to all data on the system or will the user's access be restricted?
5. What controls are in place to prevent the misuse of data by those having access?
6. Do other systems share data or have access to data in this system?
7. Who will be responsible for protecting the privacy rights of the taxpayers and employees affected by the interface?
8. Will other agencies share data or have access to data in this system?
9. How will the system ensure that agencies only get the information they are entitled?
10. How will the data be used by the agency?
11. Who is responsible for assuring proper use of the data?

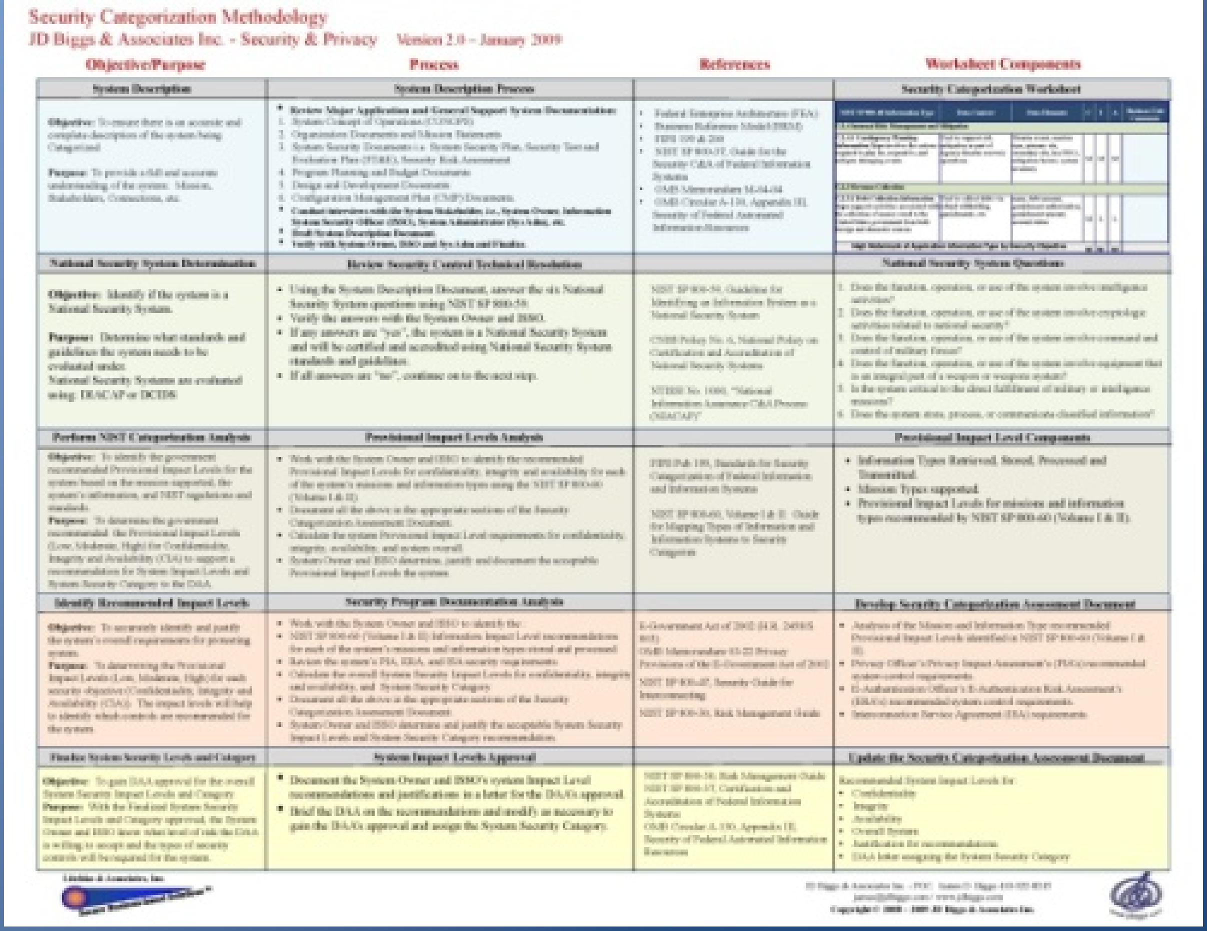
Privacy Threshold Analysis (PTA)



- Assemble Stakeholders to complete PTA (PIA - Determination)
- Apply PIA information Classification and PIA Data Access evaluation results to answer PTA questionnaire.
- Does system contain Financial Information
- Draft complete Information System Description:
  - System Boundaries
  - Evaluate Information Exchange Interconnection Security Agreements (ISA)
  - Lifecycle Status (Developing or purchasing new systems or revising current systems)
  - Define System Use and Traffic logs
- FISMA Tracking Reporting System: Yes / No
- Privacy Sensitive System: Yes / No
- National Security System: Yes / No
- Legacy System: Yes / No
- HR System: Yes / No
- Determine if PIA is required prior to submitting to Privacy Office
- Submit Draft PTA version 0.1 to Privacy Office and CC Stakeholders

Your Trusted Partner
for Improved
Security & Privacy

Security Categorization



Security Categorization Methodology
JD Biggs & Associates Inc. - Security & Privacy Version 2.0 – January 2009

Objective/Purpose	Process	References	Worksheet Components
System Description	**System Description Process**		**Security Categorization Worksheet**
Objective: To ensure there is an accurate and complete description of the system being Categorized **Purpose:** To provide a full and accurate understanding of the system: Mission, Stakeholders, Connections, etc.	▪ **Review Major Application and General Support System Documentation:** 1. System Concept of Operations (CONOPS) 2. Organization Documents and Mission Statements 3. System Security Documents i.e. System Security Plan, Security Test and Evaluation Plan (ST&E), Security Risk Assessment 4. Program Planning and Budget Documents 5. Design and Development Documents 6. Configuration Management Plan (CMP) Documents ▪ **Conduct interviews with the System Stakeholders, i.e., System Owner, Information System Security Officer (ISSO), System Administrator (Sys Adm), etc.** ▪ **Draft System Description Document.** ▪ **Verify with System Owner, ISSO and Sys Adm and Finalize.**	▪ Federal Enterprise Architecture (FEA) ▪ Business Reference Model (BRM) ▪ FIPS 199 & 200 ▪ NIST SP 800-37, Guide for the Security C&A of Federal Information Systems ▪ OMB Memorandum M-04-04 ▪ OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources	[illegible]
National Security System Determination	**Review Security Control Technical Resolution**		**National Security System Questions**
Objective: Identify if the system is a National Security System. **Purpose:** Determine what standards and guidelines the system needs to be evaluated under. National Security Systems are evaluated using: DIACAP or DCID6	▪ Using the System Description Document, answer the six National Security System questions using NIST SP 800-59. ▪ Verify the answers with the System Owner and ISSO. ▪ If any answers are "yes", the system is a National Security System and will be certified and accredited using National Security System standards and guidelines. ▪ If all answers are "no", continue on to the next step.	NIST SP 800-59, Guideline for Identifying an Information System as a National Security System CNSS Policy No. 6, National Policy on Certification and Accreditation of National Security Systems NSTISSI No. 1000, "National Information Assurance C&A Process (NIACAP)"	1. Does the function, operation, or use of the system involve intelligence activities? 2. Does the function, operation, or use of the system involve cryptologic activities related to national security? 3. Does the function, operation, or use of the system involve command and control of military forces? 4. Does the function, operation, or use of the system involve equipment that is an integral part of a weapon or weapons system? 5. Is the system critical to the direct fulfillment of military or intelligence missions? 6. Does the system store, process, or communicate classified information?
Perform NIST Categorization Analysis	**Provisional Impact Levels Analysis**		**Provisional Impact Level Components**
Objective: To identify the government recommended Provisional Impact Levels for the system based on the mission supported, the system's information, and NIST regulations and standards. **Purpose:** To determine the government recommended the Provisional Impact Levels (Low, Moderate, High) for Confidentiality, Integrity and Availability (CIA) to support a recommendation for System Impact Levels and System Security Category to the DAA.	▪ Work with the System Owner and ISSO to identify the recommended Provisional Impact Levels for confidentiality, integrity and availability for each of the system's missions and information types using the NIST SP 800-60 (Volume I & II) ▪ Document all the above in the appropriate sections of the Security Categorization Assessment Document. ▪ Calculate the system Provisional Impact Level requirements for confidentiality, integrity, availability, and system overall. ▪ System Owner and ISSO determine, justify and document the acceptable Provisional Impact Levels the system	FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems NIST SP 800-60, Volume I & II: Guide for Mapping Types of Information and Information Systems to Security Categories	▪ Information Types Retrieved, Stored, Processed and Transmitted. ▪ Mission Types supported. ▪ Provisional Impact Levels for missions and information types recommended by NIST SP 800-60 (Volume I & II).
Identify Recommended Impact Levels	**Security Program Documentation Analysis**		**Develop Security Categorization Assessment Document**
Objective: To accurately identify and justify the system's overall requirements for protecting system. **Purpose:** To determining the Provisional Impact Levels (Low, Moderate, High) for each security objective (Confidentiality, Integrity and Availability (CIA)). The impact levels will help to identify which controls are recommended for the system.	▪ Work with the System Owner and ISSO to identify the: ▪ NIST SP 800-60 (Volume I & II) Information Impact Level recommendations for each of the system's missions and information types stored and processed ▪ Review the system's PIA, ERA, and ISA security requirements ▪ Calculate the overall System Security Impact Levels for confidentiality, integrity and availability, and System Security Category ▪ Document all the above in the appropriate sections of the Security Categorization Assessment Document. ▪ System Owner and ISSO determine and justify the acceptable System Security Impact Levels and System Security Category recommendations.	E-Government Act of 2002 (H.R. 2458/S 803) OMB Memorandum 03-22 Privacy Provisions of the E-Government Act of 2002 NIST SP 800-47, Security Guide for Interconnecting NIST SP 800-30, Risk Management Guide	▪ Analysis of the Mission and Information Type recommended Provisional Impact Levels identified in NIST SP 800-60 (Volume I & II) ▪ Privacy Officer's Privacy Impact Assessment's (PIA's) recommended system control requirements ▪ E-Authentication Officer's E-Authentication Risk Assessment's (ERA's) recommended system control requirements. ▪ Interconnection Service Agreement (ISA) requirements.
Finalize System Security Levels and Category	**System Impact Levels Approval**		**Update the Security Categorization Assessment Document**
Objective: To gain DAA approval for the overall System Security Impact Levels and Category. **Purpose:** With the Finalized System Security Impact Levels and Category approved, the System Owner and ISSO know what level of risk the DAA is willing to accept and the types of security controls will be required for the system.	▪ Document the System Owner and ISSO's system Impact Level recommendations and justifications in a letter for the DAA's approval. ▪ Brief the DAA on the recommendations and modify as necessary to gain the DAA's approval and assign the System Security Category.	NIST SP 800-30, Risk Management Guide NIST SP 800-37, Certification and Accreditation of Federal Information Systems OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources	Recommended System Impact Levels for: ▪ Confidentiality ▪ Integrity ▪ Availability ▪ Overall System ▪ Justification for recommendations. ▪ DAA letter assigning the System Security Category

[illegible] & Associates, Inc.

JD Biggs & Associates Inc. – POC: James D. Biggs [illegible]
james@jdbiggs.com / www.jdbiggs.com
Copyright © 2008 – 2009 JD Biggs & Associates Inc.

JDBIGGS
Associates
Security & Privacy Consulting

Security Categorization

- Completing the Security Categorization exercise determines if a system is a *National Security System* or *Sensitive But-Unclassified*, and which baseline Security Controls are required during the Risk Assessment. This activity is required to determine the initial minimum set of Management, Operational and Technical Security Controls for both **information and information systems.**
- To complete this exercise, Stakeholders (CISO, Program Manager, ISSM, ISSO, TBD) must use the following Publications as Guidance:
  - Federal Information Processing Standards (FIPS) 199 and FIPS 200
  - National Institute of Standards Technology (NIST) Special Publication 800-53, -59, & -60

Security Categorization

- Determine Data Used By The System – List all data that is Received, Generated, Processed, Stored or Transmitted by the System
- Categorize Data into Information Types – Using NIST 800-60 Information Types
- Select Impact Rating for Information Types – Based on Information Type definitions
- Review / Adjust / Finalize and Establish Justifications for changes to default Impact Ratings (Low, Moderate, High)
- Determine National Security System Classification – Using NIST SP 800-59 (Based on the Data and System)
- Assign System Security Category – MA, GSS (Low, Moderate, High)

Security Categorization

Yes	No	National Security system Six (6) questions
□	☑	Does or Does Not Involve Intelligence Activities?
□	☑	Does or Does Not Involve Cryptographic Activities Related To National Security?
□	☑	Does or Does Not Involve Command And Control of Military Forces?
□	☑	Does or Does Not Involve Equipment That is an Integral Part of a Weapon or Weapons System?
□	☑	Is or is Not Critical to The Direct Fulfillment of Military or Intelligence Missions?
□	☑	Does or Does Not Store, Process, or Communicate Classified Information?

- NIST SP 800-59

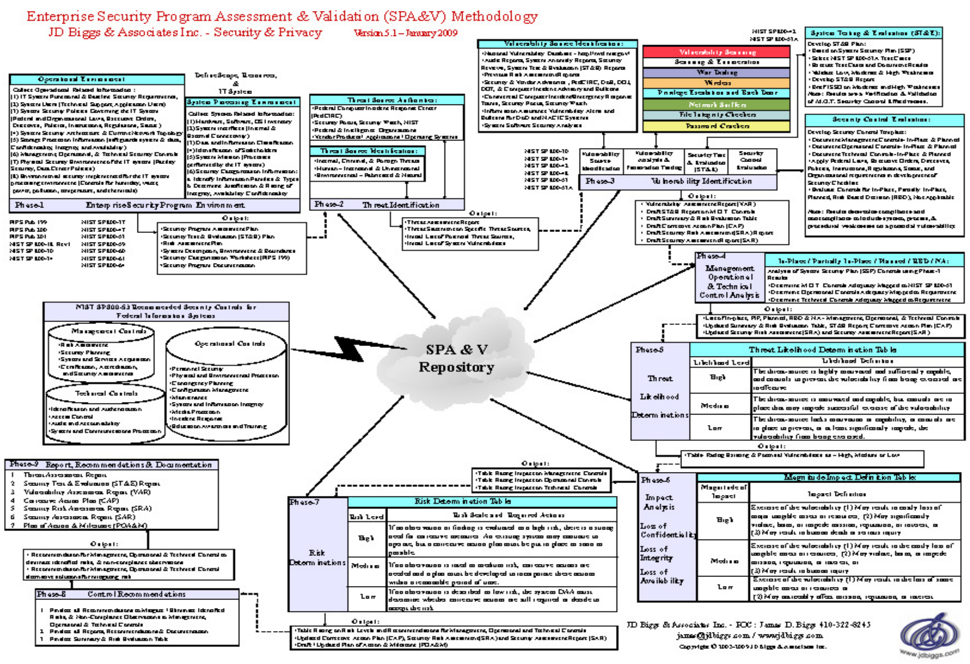
NIST SP 800-60 Information Type	Agency Data Context	Agency Data Elements	C	I	A	Business Unit Comments
C.2.1.1 Corrective Action Information Type involves the enforcement functions necessary to remedy programs that have been found non-compliant with a given law, regulation, or policy.	Used to document and resolve non-compliance issues within the Agency to ensure regulatory and policy compliance.	Program name, POC, infraction, recommended correction or mitigation, timeline, punitive action, status	**L**	**L**	**L**	
C.2.1.3 Program Monitoring Information Type involves the data-gathering activities required to determine the effectiveness of internal and external programs and the extent to which they comply with related laws, regulations, and policies.			**L**	**L**	**L**	
C.2.2.2 Public Comment Tracking Information Type involves the activities of soliciting, maintaining, and responding to public comments regarding proposed regulations.			**L**	**L**	**L**	
C.2.4.1 Contingency Planning Information Type involves the actions required to plan for, respond to, and mitigate damaging events.	Used to support risk mitigation as part of Agency disaster recovery operations.	Disaster event, reaction type, primary site, secondary site, key POCs, mitigation factors, system inventory	**M**	**M**	**H**	Disaster event information is critical to reducing human injury.
C.2.4.2 Continuity of Operations Information Type involves the activities associated with the identification of critical systems and processes, and the planning and preparation required to ensure that these systems and processes will be available after a catastrophic event.	Used to support backup server initiation procedures for critical Agency systems.	Disaster event, reaction type, primary site, secondary site, key POCs, mitigation factors, system inventory, identified critical systems	**M**	H	**M**	Disaster information procedures must be updated and accurate to reduce human injury.
Final Security Categorization for Information System			**M**	**H**	**H**	

Your Trusted Partner
for Improved
Security & Privacy

Security Program Assessment and Validation (SPA&V) Methodology

Conducting Risk Assessment on Major Applications and General Support Systems

SPA&V Methodology


Enterprise Security Program Assessment & Validation (SPA&V) Methodology
JD Biggs & Associates Inc. - Security & Privacy
Version 5.1 – January 2009
Operational Environment
Collect Operational Related Information:
(1) IT System Functional & Baseline Security Requirements,
(2) System Users (Technical Support, Application Users)
(3) System Security Policies Governing the IT System (Federal and Organizational Laws, Executive Orders, Directives, Policies, Instructions, Regulations, Status)
(4) System Security Architecture & Current Network Topology
(5) Storage Protection Information (safeguards system & data, Confidentiality, Integrity, and Availability)
(6) Management, Operational, & Technical Security Controls
(7) Physical Security Environment of the IT system (Facility Security, Data Center Policies)
(8) Environmental security implemented for the IT system processing environment (Controls for humidity, water, power, pollution, temperature, and chemicals)
Define Scope, Resources, & IT System
System Processing Environment
Collect System Related Information:
(1) Hardware, Software, OS Inventory
(2) System Interfaces (Internal & External Connectivity)
(3) Data and Information Classification
(4) Identification of Stakeholders
(5) System Mission (Processes performed by the IT system)
(6) Security Categorization Information:
a. Identify Information Providers & Types
b. Determine Justification & Rating of Integrity, Availability Confidentiality
Phase-1 Enterprise Security Program Environment
FIPS Pub 199
FIPS Pub 200
FIPS Pub 201
NIST SP 800-18, Rev1
NIST SP 800-30
NIST SP 800-34
NIST SP800-37
NIST SP800-47
NIST SP800-53
NIST SP800-59
NIST SP800-60
NIST SP800-61
NIST SP800-64
Output:
•Security Program Assessment Plan
•Security Test & Evaluation (ST&E) Plan
•Risk Assessment Plan
•System Description, Environment & Boundaries
•Security Categorization Worksheet (FIPS 199)
•Security Program Documentation
Threat Source Authorities:
•Federal Computer Incident Response Center (FedCIRC)
•Security Focus, Security Watch, NIST
•Federal & Intelligence Organizations
•Vendor Products / Applications / Operating Systems
Threat Source Identification:
•Internal, External, & Foreign Threats
•Human – Intentional & Unintentional
•Environmental – Fabricated & Natural
Phase-2 Threat Identification
Output:
•Threat Assessment Report
•Threat Statements on Specific Threat Sources,
•Initial List of Potential Threat Sources,
•Initial List of System Vulnerabilities
Vulnerability Source Identification:
•National Vulnerability Database - http://nvd.nist.gov/
•Audit Reports, System Anomaly Reports, Security Reviews, System Test & Evaluation (ST&E) Reports
•Previous Risk Assessment Reports
•Security & Vendor Advisories, FedCIRC, DoD, DOJ, DOT, & Computer Incident Advisory and Bulletins
•Commercial Computer Incident/Emergency Response Teams, Security Focus, Security Watch
•Information Assurance Vulnerability Alerts and Bulletins for DoD and NACIC Systems
•System Software Security Analyses
Vulnerability Scanning
Scanning & Enumeration
War Dialing
Wireless
Privilege Escalation and Back Door
Network Sniffers
File Integrity Checkers
Password Crackers
NIST SP800-42
NIST SP 800-53A
System Testing & Evaluation (ST&E):
Develop ST&E Plan:
•Based on System Security Plan (SSP)
•Select NIST SP 800-53A Test Cases
•Execute Test Cases and Document Results
•Validate Low, Moderate & High Weaknesses
•Develop ST&E Report
•Brief ISSO on Moderate and High Weaknesses
Note: Results are a Verification & Validation of M.O.T. Security Control Effectiveness.
NIST SP 800-30
NIST SP 800-34
NIST SP 800-42
NIST SP 800-48
NIST SP 800-53
NIST SP 800-53A
Vulnerability Source Identification
Vulnerability Analysis & Penetration Testing
Security Test & Evaluation (ST&E)
Security Control Evaluation
Phase-3 Vulnerability Identification
Output:
• Vulnerability Assessment Report (VAR)
• Draft ST&E Report on M.O.T. Controls
• Draft Summary & Risk Evaluation Table
• Draft Corrective Action Plan (CAP)
• Draft Security Risk Assessment (SRA) Report
• Draft Security Assessment Report (SAR)
Security Control Evaluation:
Develop Security Control Template:
•Document Management Controls- In-Place & Planned
•Document Operational Controls- In-Place & Planned
•Document Technical Controls- In-Place & Planned
•Apply Federal Laws, Executive Orders, Directives, Policies, Instructions, Regulations, Status, and Organizational requirements in development of Security Checklist
•Evaluate Controls for In-Place, Partially In-Place, Planned, Risk Based Decision (RBD), Not Applicable
Note: Results determine compliance and noncompliance to include system, process, & procedural weaknesses or a potential vulnerability.
Phase-4
Management, Operational & Technical Control Analysis
In-Place / Partially In-Place / Planned / RBD / NA:
Analysis of System Security Plan (SSP) Controls using Phase-1 Results
•Determine M.O.T. Controls Adequacy Mapped to NIST SP 800-53
•Determine Operational Controls Adequacy Mapped to Requirements
•Determine Technical Controls Adequacy Mapped to Requirements
Output:
•List of In-place, PIP, Planned, RBD & NA - Management, Operational, & Technical Controls
•Updated Summary & Risk Evaluation Table, ST&E Report, Corrective Action Plan (CAP)
•Updated Security Risk Assessment (SRA) and Security Assessment Report (SAR)
NIST SP800-53 Recommended Security Controls for Federal Information Systems
Management Controls
•Risk Assessment
•Security Planning
•System and Services Acquisition
•Certification, Accreditation, and Security Assessments
Technical Controls
•Identification and Authentication
•Access Control
•Audit and Accountability
•System and Communications Protection
Operational Controls
•Personnel Security
•Physical and Environmental Protection
•Contingency Planning
•Configuration Management
•Maintenance
•System and Information Integrity
•Media Protection
•Incident Response
•Education, Awareness and Training
SPA & V Repository
Phase-5
Threat Likelihood Determinations
Threat Likelihood Determination Table
Likelihood Level | Likelihood Definition
High | The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium | The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low | The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.
Output:
•Table Rating Existing & Potential Vulnerabilities as – High, Medium or Low
Phase-6
Impact Analysis
Loss of Confidentiality
Loss of Integrity
Loss of Availability
Magnitude Impact Definition Table
Magnitude of Impact | Impact Definition
High | Exercise of the vulnerability (1) May result in costly loss of major tangible assets or resources; (2) May significantly violate, harm, or impede mission, reputation, or interest; or (3) May result in human death or serious injury
Medium | Exercise of the vulnerability (1) May result in the costly loss of tangible assets or resources; (2) May violate, harm, or impede mission, reputation, or interest; or (3) May result in human injury
Low | Exercise of the vulnerability (1) May result in the loss of some tangible assets or resources or (2) May noticeably affect mission, reputation, or interest.
Output:
•Table Rating Impact on Management Controls
•Table Rating Impact on Operational Controls
•Table Rating Impact on Technical Controls
Phase-7
Risk Determinations
Risk Determination Table
Risk Level | Risk Scale and Required Actions
High | If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium | If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low | If an observation is described as low risk, the system DAA must determine whether corrective actions are still required or decide to accept the risk.
Output:
•Table Rating on Risk Levels and Recommendations for Management, Operational and Technical Controls
•Updated Corrective Action Plan (CAP), Security Risk Assessment (SRA) and Security Assessment Report (SAR)
•Draft / Updated Plan of Action & Milestone (POA&M)
Phase-8 Control Recommendations
1 Finalize all Recommendations to Mitigate / Eliminate Identified Risks, & Non-Compliance Observations to Management, Operational & Technical Controls
2 Finalize all Reports, Recommendations & Documentation
3 Finalize Summary & Risk Evaluation Table
Output:
• Recommendations for Management, Operational & Technical Controls to eliminate identified risks, & non-compliance observations
• Recommendations for Management, Operational & Technical Control alternative solutions for mitigating risk
Phase-9 Report, Recommendations & Documentation
1 Threat Assessment Report
2 Security Test & Evaluation (ST&E) Report
3 Vulnerability Assessment Report (VAR)
4 Corrective Action Plan (CAP)
5 Security Risk Assessment Report (SRA)
6 Security Assessment Report (SAR)
7 Plan of Action & Milestone (POA&M)
JD Biggs & Associates Inc. - POC : James D. Biggs 410-322-8245
james@jdbiggs.com / www.jdbiggs.com
Copyright © 2003-2009 JD Biggs & Associates Inc.
www.jdbiggs.com

JDBIGGS
Associates
Security & Privacy Consulting

SPA&V Methodology

The SPA&V Methodology was developed to graphically depict the 9 Phases / Steps, facilitate the completion of each phase, and allow *Stakeholders* a Criteria to Measure the Performance of *Internal* and *Contractor Resources*.

- Phase 1 Enterprise Security Program Environment
- Phase 2 Threat Identification
- Phase 3 Vulnerability Identification
- Phase 4 Management, Operational, & Technical Control Analysis
- Phase 5 Threat Likelihood Determination
- Phase 6 Impact Analysis
- Phase 7 Risk Determination
- Phase 8 Control Recommendation
- Phase 9 Report, Recommendations and Determinations

SPA&V Methodology

- Establish a File Server as the SPA&V Repository for System Security Program Documentation:
  - Maintain Integrity, Confidentiality and Availability
- Protect the Sensitivity of these Documents using Encryption
- Identify all Stakeholders:
  - Personnel & Physical Security, Administrators, NOC / SOC…
- Evaluate the Artifacts Produced from each Phase Output
  - Accuracy, Completeness,
- Work W/Updated Security Documentation and Templates
- Must Use Current Release of C&A Management Tool

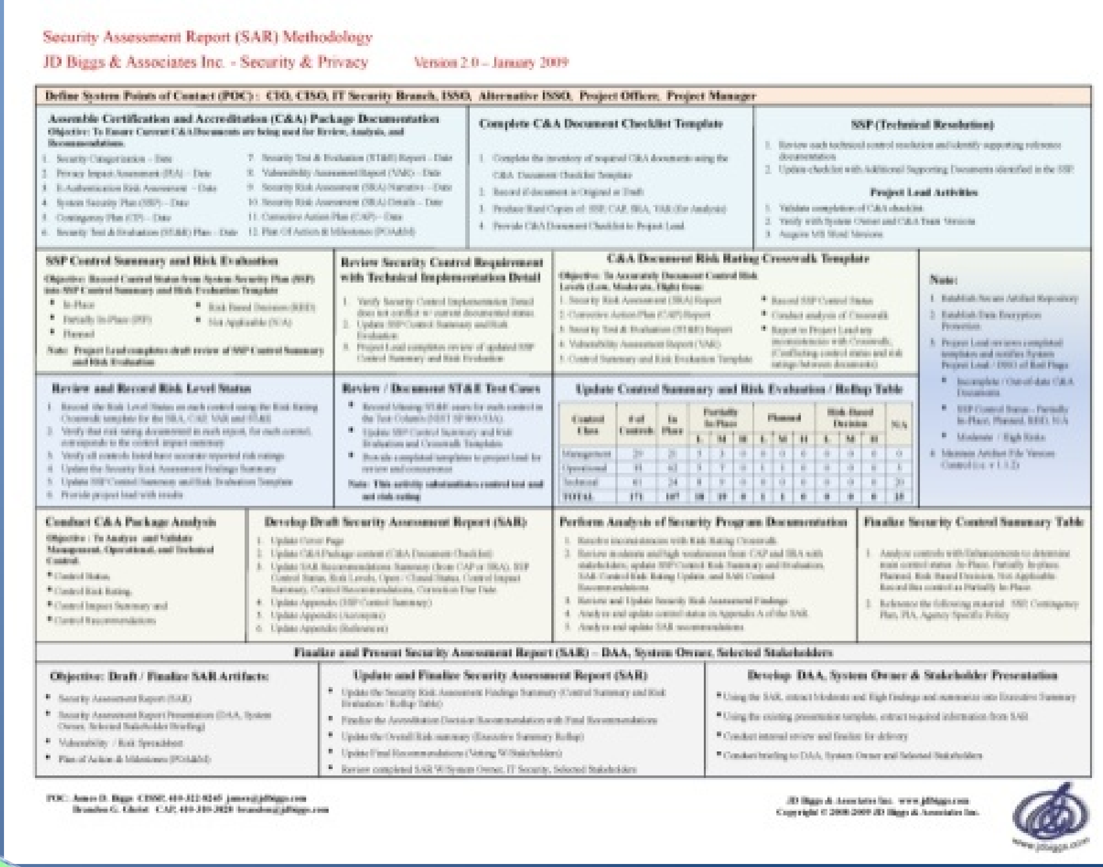
SPA&V Methodology

Each phase consists of Activities, Guidance Documentation and Tangible Outputs that Stakeholders can use for *Project / Cost / Resource* planning.

- Phase 1 Enterprise Security Program Environment
  - OUTPUT: Security Program Assessment Plan, Security Test & Evaluation Plan, Risk Assessment Plan, System Description, Categorization and Documentation
- Phase 2 Threat Identification
  - OUTPUT: Threat Assessment Report, Threat Statement on Specific Threat Sources, Initial List of Potential Threat Sources and Vulnerabilities
- Phase 3 Vulnerability Identification
  - OUTPUT: Vulnerability Assessment Report, Draft Report; ST&E / Corrective Action Plan / Security Risk Assessment / Security Assessment Report
- Phase 4 Management Operational and Technical Control Analysis
  - OUTPUT: List of In-Place / Partially In-Place / Planned / RBD / NA Controls

Your Trusted Partner
for Improved
Security & Privacy

Security Assessment Report (SAR) Methodology



Security Assessment Report (SAR) Methodology

JD Biggs & Associates Inc. - Security & Privacy Version 2.0 – January 2009

Define System Points of Contact (POC) : CIO, CISO, IT Security Branch, ISSO, Alternative ISSO, Project Officer, Project Manager

Assemble Certification and Accreditation (C&A) Package Documentation
Objective: To Ensure Current C&A Documents are being used for Review, Analysis, and Recommendations.

1. Security Categorization – Date
2. Privacy Impact Assessment (PIA) – Date
3. E-Authentication Risk Assessment – Date
4. System Security Plan (SSP) – Date
5. Contingency Plan (CP) – Date
6. Security Test & Evaluation (ST&E) Plan – Date
7. Security Test & Evaluation (ST&E) Report – Date
8. Vulnerability Assessment Report (VAR) – Date
9. Security Risk Assessment (SRA) Narrative – Date
10. Security Risk Assessment (SRA) Details – Date
11. Corrective Action Plan (CAP) – Date
12. Plan Of Action & Milestones (POA&M)

Complete C&A Document Checklist Template

1. Complete the inventory of required C&A documents using the C&A Document Checklist Template
2. Record if document is Original or Draft
3. Produce Hard Copies of: SSP, CAP, SRA, VAR (for Analysis)
4. Provide C&A Document Checklist to Project Lead

SSP (Technical Resolution)

1. Review each technical control resolution and identify supporting reference documentation
2. Update checklist with Additional Supporting Documents identified in the SSP

Project Lead Activities

1. Validate completion of C&A checklist
2. Verify with System Owner and C&A Team Versions
3. Acquire MS Word Versions

SSP Control Summary and Risk Evaluation

Objective: Record Control Status from System Security Plan (SSP) into SSP Control Summary and Risk Evaluation Template

- In-Place
- Partially In-Place (PIP)
- Planned
- Risk Based Decision (RBD)
- Not Applicable (N/A)

Note: **Project Lead completes draft review of SSP Control Summary and Risk Evaluation**

Review Security Control Requirement with Technical Implementation Detail

1. Verify Security Control Implementation Detail does not conflict w/ current documented status
2. Update SSP Control Summary and Risk Evaluation
3. Project Lead completes review of updated SSP Control Summary and Risk Evaluation

C&A Document Risk Rating Crosswalk Template

Objective: To Accurately Document Control Risk Levels (Low, Moderate, High) from:

1. Security Risk Assessment (SRA) Report
2. Corrective Action Plan (CAP) Report
3. Security Test & Evaluation (ST&E) Report
4. Vulnerability Assessment Report (VAR)
5. Control Summary and Risk Evaluation Template

- Record SSP Control Status
- Conduct analysis of Crosswalk
- Report to Project Lead any inconsistencies with Crosswalk (Conflicting control status and risk ratings between documents)

Note:

1. Establish Secure Artifact Repository
2. Establish Data Encryption Protection
3. Project Lead reviews completed templates and notifies System Project Lead / ISSO of Red Flags
   - Incomplete / Out-of-date C&A Documents
   - SSP Control Status – Partially In-Place, Planned, RBD, N/A
   - Moderate / High Risks
4. Maintain Artifact File Version Control (i.e. v 1.1.2)

Review and Record Risk Level Status

1. Record the Risk Level Status on each control using the Risk Rating Crosswalk template for the SRA, CAP, VAR and ST&E
2. Verify that risk rating documented in each report, for each control, corresponds to the control impact summary
3. Verify all controls listed have accurate reported risk ratings
4. Update the Security Risk Assessment Findings Summary
5. Update SSP Control Summary and Risk Evaluation Template
6. Provide project lead with results

Review / Document ST&E Test Cases

- Record Missing ST&E cases for each control in the Test Column (NIST SP 800-53A)
- Update SSP Control Summary and Risk Evaluation and Crosswalk Templates
- Provide completed templates to project lead for review and concurrence

Note: **This activity substantiates control test and risk rating**

Update Control Summary and Risk Evaluation / Rollup Table

Control Class	# of Controls	In Place	Partially In Place			Planned			Risk Based Decision			N/A
			L	M	H	L	M	H	L	M	H	
Management	29	21	1	1	0	0	0	0	0	0	0	0
Operational	81	62	1	7	0	1	1	0	0	0	0	1
Technical	61	24	8	9	0	0	0	0	0	0	0	20
TOTAL	171	107	10	17	0	1	1	0	0	0	0	15

Conduct C&A Package Analysis

Objective : To Analyze and Validate Management, Operational, and Technical Control.

- Control Status,
- Control Risk Rating,
- Control Impact Summary and
- Control Recommendations

Develop Draft Security Assessment Report (SAR)

1. Update Cover Page
2. Update C&A Package content (C&A Document Checklist)
3. Update SAR Recommendations Summary (from CAP or SRA), SSP Control Status, Risk Levels, Open / Closed Status, Control Impact Summary, Control Recommendations, Correction Due Date
4. Update Appendix (SSP Control Summary)
5. Update Appendix (Acronyms)
6. Update Appendix (References)

Perform Analysis of Security Program Documentation

1. Resolve inconsistencies with Risk Rating Crosswalk
2. Review moderate and high weaknesses from CAP and SRA with stakeholders; update SSP Control Risk Summary and Evaluation, SAR Control Risk Rating Update, and SAR Control Recommendations
3. Review and Update Security Risk Assessment Findings
4. Analyze and update control status in Appendix A of the SAR
5. Analyze and update SAR recommendations

Finalize Security Control Summary Table

1. Analyze controls with Enhancements to determine main control status: In-Place, Partially In-place, Planned, Risk Based Decision, Not Applicable. Record this control as Partially In-Place
2. Reference the following material: SSP, Contingency Plan, PIA, Agency Specific Policy

Finalize and Present Security Assessment Report (SAR) – DAA, System Owner, Selected Stakeholders

Objective: Draft / Finalize SAR Artifacts:

- Security Assessment Report (SAR)
- Security Assessment Report Presentation (DAA, System Owner, Selected Stakeholder Briefing)
- Vulnerability / Risk Spreadsheet
- Plan of Action & Milestones (POA&M)

Update and Finalize Security Assessment Report (SAR)

- Update the Security Risk Assessment Findings Summary (Control Summary and Risk Evaluation / Rollup Table)
- Finalize the Accreditation Decision Recommendation with Final Recommendations
- Update the Overall Risk summary (Executive Summary Rollup)
- Update Final Recommendations (Voting W/Stakeholders)
- Review completed SAR W/System Owner, IT Security, Selected Stakeholders

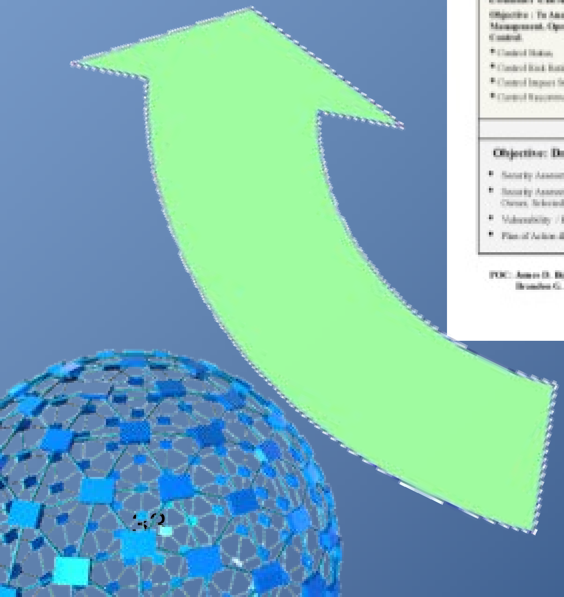
Develop DAA, System Owner & Stakeholder Presentation

- Using the SAR, extract Moderate and High findings and summarize into Executive Summary
- Using the existing presentation template, extract required information from SAR
- Conduct internal review and finalize for delivery
- Conduct briefing to DAA, System Owner and Selected Stakeholders

POC: James D. Biggs CISSP, 410-322-8245 james@jdbiggs.com
Brandon G. Christ CAP, 410-310-3820 brandon@jdbiggs.com

JD Biggs & Associates Inc. www.jdbiggs.com
Copyright © 2008-2009 JD Biggs & Associates Inc.

www.jdbiggs.com



JDBIGGS
Associates
Security & Privacy Consulting

Security Assessment Report (SAR) Methodology

The SAR is produced to brief the Designated Approving Authority(s) (DAA), System Owner and other Stakeholders on Moderate and High Risks and Recommendations within a system.

Security Program Documentation is reviewed when producing the SAR:

- Vulnerability Assessment Report (VAR),
- System Security Plan (SSP),
- ST&E Report ,
- Corrective Action Plan (CAP),
- Risk Assessment Report (SRA),
- Plan of Action & Milestone (POA&M) and other System Related Documents.

Risk Rating Crosswalk

Control		SSP	ST&E	SRA	VAR	CAP
Risk Assessment (RA)			Management			
RA-1	Risk Assessment Policy and Procedures	RBD		Moderate		Low
RA-2	Security Categorization	In Place				
RA-3	Risk Assessment	In Place				
RA-4	Risk Assessment Update	In Place		Moderate		Moderate
RA-5	Vulnerability Scanning	In Place				

SSP	System Security Plan
ST&E	Security Test and Evaluation
SRA	Security Risk Assessment
VAR	Vulnerability Assessment Report
CAP	Corrective Action Plan

Creating the Security Assessment Report (SAR)

- Conduct C&A Package Analysis of Security Program Documentation:
  - Control Status: In Place / Partially In Place / Planned / RBD / NA
  - Control Risk Rating: Low, Moderate, High
  - Control Recommendations
  - Control Implementation Description (Satisfy Requirement)
- Conduct Validation of *Moderate* and *High* Reported Weaknesses with Stakeholders and determine Legitimacy
- Conduct Stakeholder Briefings (System Owner / CISO / IT Security Branch) prior to DAA Presentation
- Finalize and Present Security Assessment Report to DAA

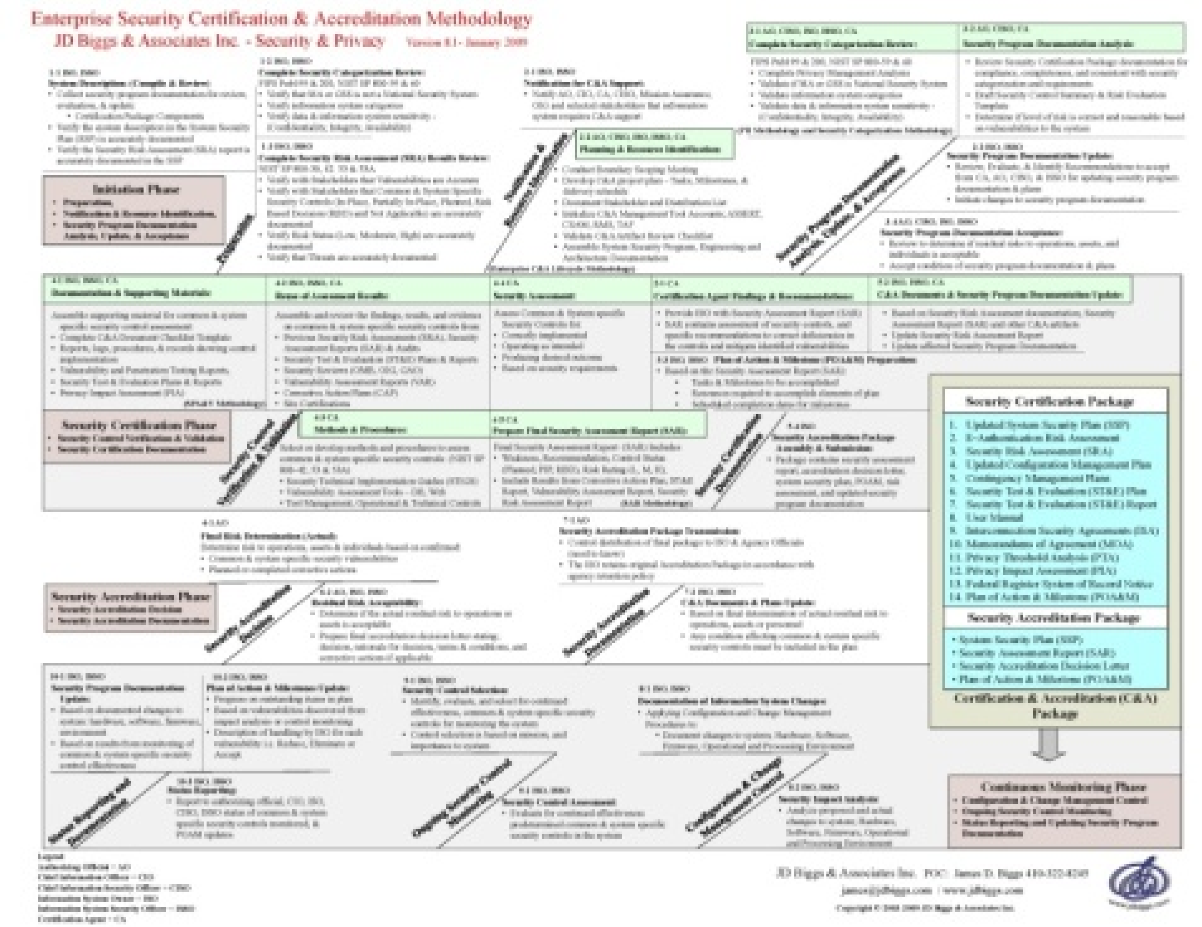
Security Control Summary & Risk Evaluation Table

Control		In Place	Partially In-Place	Planned	Risk Based Decision	Not Applicable
Risk Assessment (RA)				Management		
RA-1	Risk Assessment Policy and Procedures				X	
RA-2	Security Categorization	X				
RA-3	Risk Assessment		X			
RA-4	Risk Assessment Update	X				
RA-5	Vulnerability Scanning	X				

Control Implementation Summary

Control Family	# of Controls	In Place	Partially In Place			Planned			Risk-Based Decision			N/A
			L	M	H	L	M	H	L	M	H	
Management	29	26	-	1	-		2	-	-	-	-	-
Operational	81	64	3	5	-	2	2	-	-	-	-	5
Technical	61	33	3	5	-	-	-	-	-	-	-	20
TOTAL	171	123	6	11	-	2	4	-	-	-	-	25

Certification & Accreditation (C&A) Methodology



Enterprise Security Certification & Accreditation Methodology

JD Biggs & Associates Inc. - Security & Privacy Version 8.1 - January 2009

System Description (Compile & Review)

Complete Security Categorization Review

Notification for C&A Support

Complete Security Categorization Review

Security Program Documentation Analysis

Complete Security Risk Assessment (SRA) Results Review

Planning & Resource Identification

Security Program Documentation Update

Security Program Documentation Acceptance

Initiation Phase

- Preparation
- Notification & Resource Identification
- Security Program Documentation Analysis, Update, & Acceptance

Documentation & Supporting Materials

Reuse of Assessment Results

Security Assessment

Certification Agent Findings & Recommendations

C&A Documents & Security Program Documentation Update

Plan of Action & Milestones (POA&M) Preparation

Security Certification Phase

- Security Control Verification & Validation
- Security Certification Documentation

Methods & Procedures

Prepare Final Security Assessment Report (SAR)

Security Accreditation Package Assembly & Submission

Final Risk Determination (Actual)

Security Accreditation Package Transmission

Security Accreditation Phase

- Security Accreditation Decision
- Security Accreditation Documentation

Residual Risk Acceptability

C&A Documents & Plans Update

Security Program Documentation Update

Plan of Action & Milestones Update

Security Control Selection

Documentation of Information System Changes

Status Reporting

Security Control Assessment

Security Impact Analysis

Security Certification Package

1. Updated System Security Plan (SSP)
2. E-Authentication Risk Assessment
3. Security Risk Assessment (SRA)
4. Updated Configuration Management Plan
5. Contingency Management Plans
6. Security Test & Evaluation (ST&E) Plan
7. Security Test & Evaluation (ST&E) Report
8. User Manual
9. Interconnection Security Agreements (ISA)
10. Memorandums of Agreement (MOA)
11. Privacy Threshold Analysis (PTA)
12. Privacy Impact Assessment (PIA)
13. Federal Register System of Record Notice
14. Plan of Action & Milestones (POA&M)

Security Accreditation Package

- System Security Plan (SSP)
- Security Assessment Report (SAR)
- Security Accreditation Decision Letter
- Plan of Action & Milestones (POA&M)

Certification & Accreditation (C&A) Package

Continuous Monitoring Phase

- Configuration & Change Management Control
- Ongoing Security Control Monitoring
- Status Reporting and Updating Security Program Documentation

Legend
Authorizing Official – AO
Chief Information Officer – CIO
Chief Information Security Officer – CISO
Information System Owner – ISO
Information System Security Officer – ISSO
Certification Agent – CA

JD Biggs & Associates Inc. POC: James D. Biggs 410-322-8249
james@jdbiggs.com | www.jdbiggs.com
Copyright © 2008-2009 JD Biggs & Associates Inc.

JDBIGGS
Associates
Security & Privacy Consulting

Enterprise Security C&A Methodology

- C&A activities performed on *National Security* and *Sensitive But-Unclassified* systems are Complex, Time-Consuming and Resource Intensive.
- These activities involve reviewing of Security Program Documentation, Testing of Management, Operational and Technical Security Controls, and producing Mitigation Recommendations.
- This Methodology was Assembled using Federal Standards and designed to assist the C&A Team / Stakeholders in complying with these standards to produce the Certification Package, Accreditation Package and Security Program Documentation.

Enterprise Security C&A Methodology

- The Four Phases (Initiation, Certification, Accreditation and Continuous Monitoring) are performed using Internal and Contractor Resources. The Green Bar represents the ***Certification Agent*** activities (independent).

Initiation Phase

- Preparation
- Notification & Resource Identification
- Security Program Documentation (CA)
- Analysis, Update, & Acceptance (CA)

Security Accreditation Phase

- Security Accreditation Decision
- Security Accreditation Documentation

Security Certification Phase

- Security Control Verification & Validation (CA)
- Security Certification Documentation (CA)

Continuous Monitoring Phase

- Configuration & Change Management Control
- Ongoing Security Control Monitoring
- Status Reporting and Updating Security Program Documentation

Strategies and Methodologies for Security & Privacy Professionals

- Strategies and Methodologies:
  - – Baseline for Systems, Applications, Development and Production Environments
  - – Develop / Refine Policies, Procedures, Templates and Guidance Docs
- Educate and Train Stakeholders (Internal & Contractor Resources):
  - – System Owners, Program Managers
  - – Human Resources, Personnel and Physical Security, CO and COTR
  - – Administrators – Application / Database / Web / Firewall
  - – Security and Privacy Professionals

Your Trusted Partner
for Improved
Security & Privacy

Contract Vehicles

Schedule 70 - JD Biggs & Associates is approved for Cooperative Purchasing and can be used by Federal, State, and Local Government Agencies. Email *info@jdbiggs.com* for additional information, or to inquire about contract support / awards.

DUNS: 180401478 CAGE: 4V6P7

NAICS Codes: 541519 541512 541990

GSA Schedule 70 Contract #: GS-35F-0064V

MD SDAT ID #: D07929995

Small Business Reserve: SB08-3618

eMaryland Marketplace ID #: 264705

www.jdbiggs.com

JD Biggs & Associates, Inc.
12602 Bear Creek Terrace
Beltsville, MD 20705
Voice: (410) 322-8245 Fax: (301) 560-8431

Contacts:

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

Suzanne Biggs, CAP
Office Manager/Principal Consultant
443-484-2723
suzanne@jdbiggs.com

Sara Ghrist
Human Resources Consultant
443-745-8276
sara@jdbiggs.com

JDBIGGS
Associates
Security & Privacy Consulting