Electrosoft

Perspectives on FedRAMP

Dr. Sarbari Gupta, CISSP, CISA

Electrosoft Services, Inc.
1893 Metro Center Drive
Suite 228
Reston, VA 20190

Web: http://www.electrosoft-inc.com
Email: info@electrosoft-inc.com
Tel: (703) 437-9451
FAX: (703) 437-9452

Electrosoft Corporate Overview

- **Management and Technology Services Firm**
  - **Focus on Identity Management and Cybersecurity**
- **Serving Federal / Commercial Customers since 2001**
- **Located in the National Capital Region**
- **Small Business Certifications**
  - **Small Disadvantaged Business (SBA SDB)**
  - **Economically Disadvantaged Woman-Owned (SBA EDWOSB)**
  - **Minority-Owned (VA SWAM)**
- **Mature Organization and Processes**
  - **ISO 9001:2008**
  - **CMMI Level 2**

Sample FedRAMP / FISMA Experience

Customer	Target System	Description
Commercial Cloud Service Providers (CSP)	Multiple Cloud Services	• FedRAMP Readiness Reviews for multiple CSPs • Assist CSPs with FedRAMP Preparation • FedRAMP Assessments and Penetration Testing
CLW	Cloud Infrastructure as a Service (IaaS)	• Prepare full set of System Owner documents including SSP, IT Contingency Plan, Configuration Mgmt Plan, IR Plan, Continuous Monitoring Plan • Security Control Assessment with Penetration Testing
VA OI&T OSP	Enterprise Physical Access Control System (ePACS)	• Prepare full set of System Owner documents including SSP, IT Contingency Plan, Configuration Mgmt Plan, IR Plan, Continuous Monitoring Plan • Select/Implement security controls
Experian	Precise ID (PID) System	• Full Security Control Assessment of the PID System
Global Patent Solutions	Automated Information Management System (AIMS)	• Security Assessment of target system • Prepare POA&M • Assemble Security Authorization Package
DOC USPTO	More than 40 General Support Systems and Major Applications	• IV&V Review of C&A Packages • Remediation Oversight • Continuous Monitoring
National Gallery of Art	General Support System (GSS) and all Major Applications (MA)	• Full C&A for NGA GSS and all MAs • Develop Database for POA&M Tracking • Develop Security Policies and Procedures

Other Relevant Experience

- **NIST Cybersecurity Subject Matter Expert**
  - Supported development of NIST Smart Card standard (FIPS 201)
  - Co-authorship of several NIST Special Publications, including
    - SPs 800-63-2, 800-79-1, 800-128, 800-85B, 800-73-4, 800-157, and others
- **Serving Federal Government Cybersecurity Projects for 11 years**
  - FISMA and FedRAMP Services
  - Identity and Access Management
  - Health IT Security and Privacy
- **Kantara Identity Assurance Framework Assessor**
  - One of only 4 accredited assessors
  - Completed successful audit of Experian, Symantec and Aetna
- **Public Key Infrastructure (PKI) Audits**
  - Department of State PKI
  - Treasury Shared Service Provider (SSP) PKI
  - Exostar Shared Service Provider (SSP) PKI

FedRAMP 3PAO Certification Experience

- **Initial Submission for 3PAO – 01/2012**
- **Two rounds of Feedback on Deficiencies**
  - **ISO 17020 Conformance**
  - **Use of FedRAMP Templates**
- **Achieve 3PAO Accreditation – 08/2012**
- **Thoughts on the Process:**
  - **Stringent on Independence of Assessor**
  - **No cost/fee involved**

Upcoming A2LA 3PAO Certification

- **3PAO Accreditation transitioned to A2LA**
  - **As of 03/2013**
  - **A2LA – American Association for Laboratory Accreditation**
- **Electrosoft preparing for A2LA Re-accreditation**
  - **Target date – 07/2014**
- **Thoughts on the Process:**
  - **Significant cost/fee involved**
  - **Onsite inspection**
  - **Lots of paperwork and assertions**

Market for 3PAO Assessments

- **Market / Demand has been quite lean**
  - **Average of 2-4 inquiries per month**
- **Many inquiries are for FedRAMP consulting**
- **CSPs looking for education on FedRAMP**
- **Many CSPs deciding to wait for market demand**
- **Government customer frequently unwilling to pick up FedRAMP costs**

What we hear from our CSP Clients …

CSPs have grossly underestimated …

- **FedRAMP effort**
  - **Extensive documentation**
  - **Depth and breadth of the security controls**
  - **Extreme rigor of the FedRAMP process**
  - **Subjectivity of security control interpretations**
    - o
- **FedRAMP Authorization cost**
  - **Internal costs to develop documents**
  - **Costs for additional security control implementation**
  - **Cost for 3PAO assessment**
  - **Cost of continuous monitoring**
- **FedRAMP Authorization timeline**
  - **Minimum of 6-9 months after FedRAMP docs are ready**

FedRAMP Statistics – 03/2014

- **FedRAMP JAB Authorization (total of 12 CSPs):**
  - **IaaS – 9 CSPs**
  - **PaaS – 2 CSPs**
  - **SaaS – 1 CSP**
- **FedRAMP Agency Authorization (total of 3 CSPs):**
  - **Iaas – 2 CSPs**
  - **SaaS – 1 CSP**
- **FedRAMP Pending Pipeline – CSPs at each stage:**
  - **Documentation Phase – 12**
  - **Testing Phase – 3**
- **3PAO Assessment Cost – Median $250**
  - **Range of $200K – $5M**

- **Source:** http://www.meritalk.com/fedramp.php

Electrosoft Perspectives as 3PAO

- FedRAMP templates and processes mature
- Insufficient market demand
- FedRAMP program undergoing change
- JAB Authorization intrinsically different from Agency Authorization
  - Agency Authorization is risk-based with view to mission
  - JAB has very low risk tolerance – no mission view
- Few examples and lessons-learned available

Concluding Remarks

- **Extreme rigor and cost of FedRAMP JAB Authorization may slow cloud adoption by Agencies**
  - **Delays disruptive to achieving mission needs**
  - **Costs very high (unless amortized across many Agencies)**
- **FedRAMP Agency Authorization may represent more cost-effective approach in the near-term**
  - **Agencies can take risk-based approach to authorization**
- **Many CSPs waiting for dust to settle before embarking on grueling path to FedRAMP**
- **Contact information:**
  - **Dr. Sarbari Gupta. CISSP, CISA, CAP – President & CEO**
    - **sarbari@electrosoft-inc.com**
    - **703-437-9451 ext 12**