

Transforming the SRS Cyber Security Program

Juli Hearn, CISSP

Principal Cyber Security Engineer

Savannah River Nuclear Solutions, LLC
April 2012

DOE Information Management Conference

Dallas, Texas

Savannah River Nuclear Solutions



SRNS is the M&O contractor for DOE's Savannah River Site in Aiken, S.C.

The primary initiatives for SRNS are national security, clean energy and environmental stewardship.

- We provide nuclear materials management to support national defense and U.S. nuclear nonproliferation efforts.
- We support the National Nuclear Security Administration by extracting tritium and delivering products to military and weapons design agencies.
- We develop and deploy environmental cleanup technologies.
- We conduct technology R&D on national energy independence initiatives.

[\(Click to Skip this Advertisement\)](#)



Agenda

- **Background**
 - About SRS
 - Diversity of Tenants
- **CS Program Transformation**
 - Capitalizing on Commonality
 - Managing Risk
 - From “Many” to “One”
- **Foundation for the Future**
 - Mission Based RMF
 - Integrated Cyber Security
 - Enterprise SRS
- **Wrap Up**



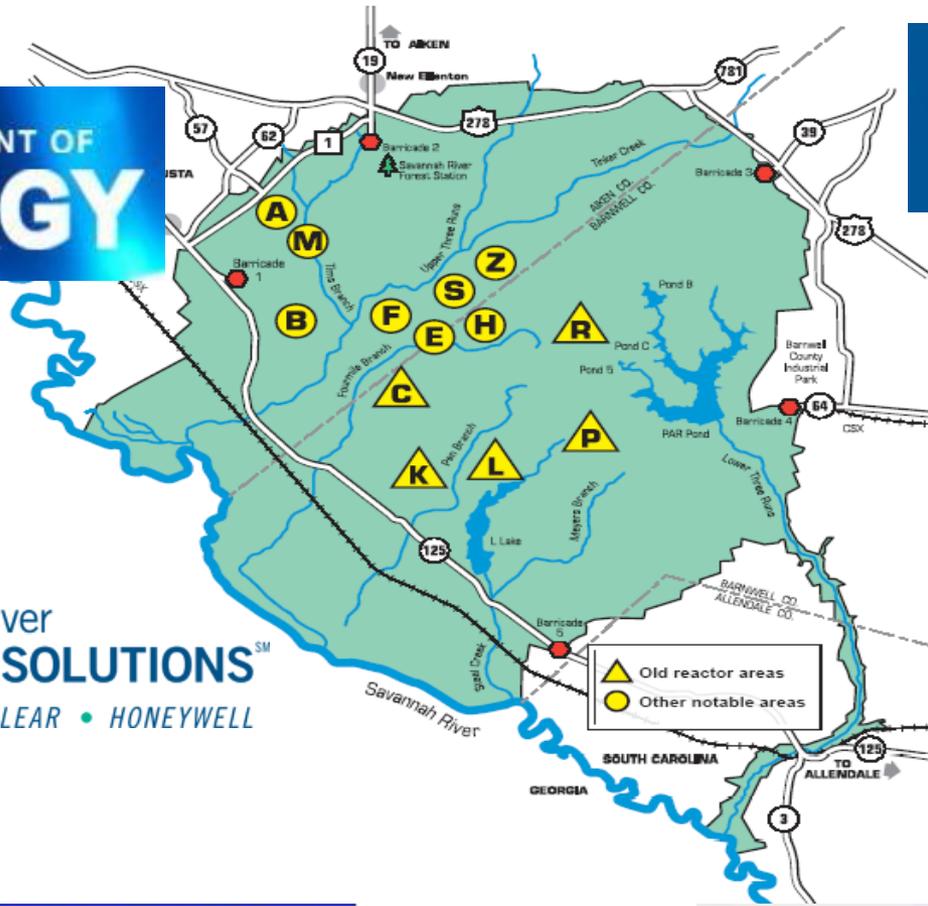
Savannah River Site – SRS Background



- Covers 198,344 Acres, 310 Square Miles
- Inhabits Portions of Aiken, Barnwell, and Allendale Counties in South Carolina
- Lines 17 Miles Savannah River Frontage
- Includes 13 Main Facility Areas

Fun Fact: The entire Washington, DC area will fit inside the SRS boundary.

Savannah River Site - SRS



SRS Cyber Security Program History

- **Multiple Tenants with Separate Programs**
- **Inefficiencies, Duplication of Effort, Lack of Security Focus**
- **Cyber Security not Integrated into the Business**
- **Level of Risk not Quantifiable / Manageable**
- **2006 IG Audit finding – No Cyber Security Program, Requirements Not Met.**



Transformation – Capitalizing on Commonality

- **Common Requirements**
 - DOE Order 205.1A
 - PCSP 1.1
 - CNSSI 1253
 - NIST 800-53, Rev. 1
 - FIPS 199 Security Categorization
- **Common Infrastructure**
 - Site Network
 - Centralized IT management
 - M&O Cyber Security Organization
- **Common Controls**
 - Moderate Level Categorization
 - 80% Rule
 - As an “Umbrella” Accreditation Boundary
 - Inheritance Approach

Common Controls Development and Implementation

- **Inheritance Approach**
 - Accreditation Boundary SSP
 - Project SSPs rolled up
 - Narrative portion showing controls inheritance
 - Difference (from Common Control implementation)
 - Deviation (from PCSP requirement – Variance or Waiver)
 - Tailoring (for PC systems)
 - MOTs tables for Differences / Deviations Only
 - Configuration Management Plan, Contingency Plan as attachments
 - Deviation Documentation
 - Variance: DAA Acceptance
 - Waiver: DOE HQ CSPM Acceptance
 - ST&E
 - AB Testing focused on controls not inherited
- **Baseline Approach (Classified)**
 - Accreditation Boundary SSP
 - One for each distinct system
 - MOTs tables for all Controls
 - ST&E
 - All controls tested

| Control | Inherited | Status |
|---------|-----------|--|
| AC-2 | No | Meet Control Program Implementation Variance |
| AC-3 | No | Meet Control Program Implementation Variance |
| AC-4 | Yes | |
| AC-5 | No | Meet Control Program Implementation Variance |
| AC-6 | Yes | |
| AC-7 | No | Control is Partially Implemented Compensatory Measures / Waiver Request |

Transformation – Managing Risk

- **Accreditation Boundary Structure**
 - Evolution of Three to Eleven to Six
 - Focus on Functionality, Financial Responsibility, Organizational Structure
- **Differences and Deviations**
 - Documented in SSPs
 - Identification of Risk
 - Mitigations / Acceptance
 - POA&Ms
- **Additional Benefits**
 - Development of Comprehensive DR / CP Plans
 - Unified Configuration Management
 - *Approved Security Configuration Baselines (eg., FDCC)*
 - *CCRB*
 - Integration of Cyber Security within Business / Mission and Lifecycle

SRS Accreditation Boundary Structure

EM Unclassified

- **Common Controls AB**
 - Security Systems Sub-AB
 - Infrastructure Sub-AB
 - Enterprise Applications Sub-AB
 - SRNL Sub-AB
 - Open / Public Access Sub-AB
- **E&PC AB**
- **Federal Systems AB**
- **WSI AB**
- **SRR AB**
- **SWPF AB**

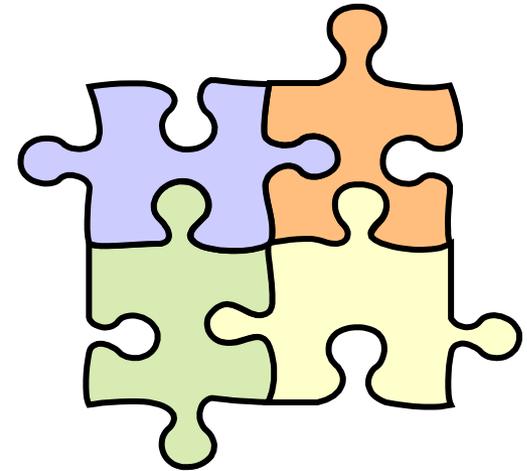
EM and NNSA Classified

- **Baseline Controls Document**
 - SSP for each system /network

MOX - Separate Network and Program

Transformation – From Many to One

- **Vulnerability and Patch Management Team**
- **Cyber Security Configuration Management Team and Firewall Configuration Management Team**
- **Risk Management**
 - Controlled Hardware and Software
 - Risk Entry Application
 - Telecom Proposals
 - Risk Assessments
- **Incident Response**
 - Tie-in to DR / CP
- **Audits and Data Calls**
- **Continuous Monitoring**
- **Realized Program Efficiencies Through Shared Efforts**
- **Improved Cyber Security for the Enterprise**



Foundation for the Future

- **Supports Paradigm shift – From Compliance Based to Securing Systems**
 - Documentation as a By-product
 - Implementation of Automated Processes and Monitoring
 - Development and Use of Meaningful Metrics
- **Implementation of RMF – Based on / Supporting Mission(s)**
- **Incorporation of Governance Process**
- **Capability for More Rapid Assessment and Deployment of New Technology**
- **Ensures Identification and Acceptance of Risk**
- **Flexibility for Enterprise Level Support**
 - Incorporation of Other Tenants – NNSA, MOX
 - Supports the Future Vision for the Site



Wrap Up - SRS Cyber Security Program Transformation

- **Developed Site-wide, Cross-tenant Partnerships**
- **Created and Implemented a Common Framework**
 - Meeting Requirements
 - Minimal Risk
- **Achieves Common Goals**
 - Integrated Security for Systems and Data Protection
 - Management of Risks
 - Secure Deployment of New Technologies
- **Provides the Foundation for New Enterprise-level Endeavors**