Savannah River National Laboratory®

OPERATED BY SAVANNAH RIVER NUCLEAR SOLUTIONS

We put science to work.™

CYBER SECURITY AT THE NATIONAL LABS

A Brief Overview with Emphasis on SRNL

A government contractor's perspective

Steven L. Tibrea,

Chief Information Officer

USC / NSF Workshop

July 23, 2017

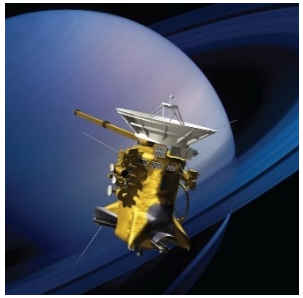
Savannah River NUCLEAR SOLUTIONS℠

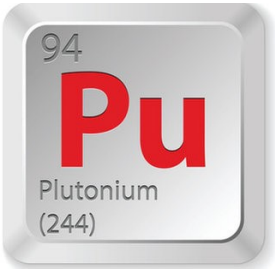
FLUOR • NEWPORT NEWS NUCLEAR • HONEYWELL

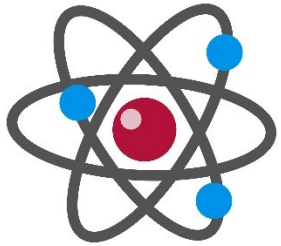
The Manhattan Project: Birth of the National Labs

75 Years of National Laboratory Breakthroughs

- Decoded DNA
- Powered NASA spacecraft
- Confirmed the Big Bang and discovered dark energy
- Unmasked a dinosaur killer
- Detected the neutrino
- Discovered gamma ray bursts
- Discovered 22 elements
- Pioneered optical digital recording (CDs, DVDs)
- Locked nuclear waste in glass
- Launched the LED lighting revolution
- Harnessed the power of the atom
- Made wind power mainstream







Office of Science Laboratories

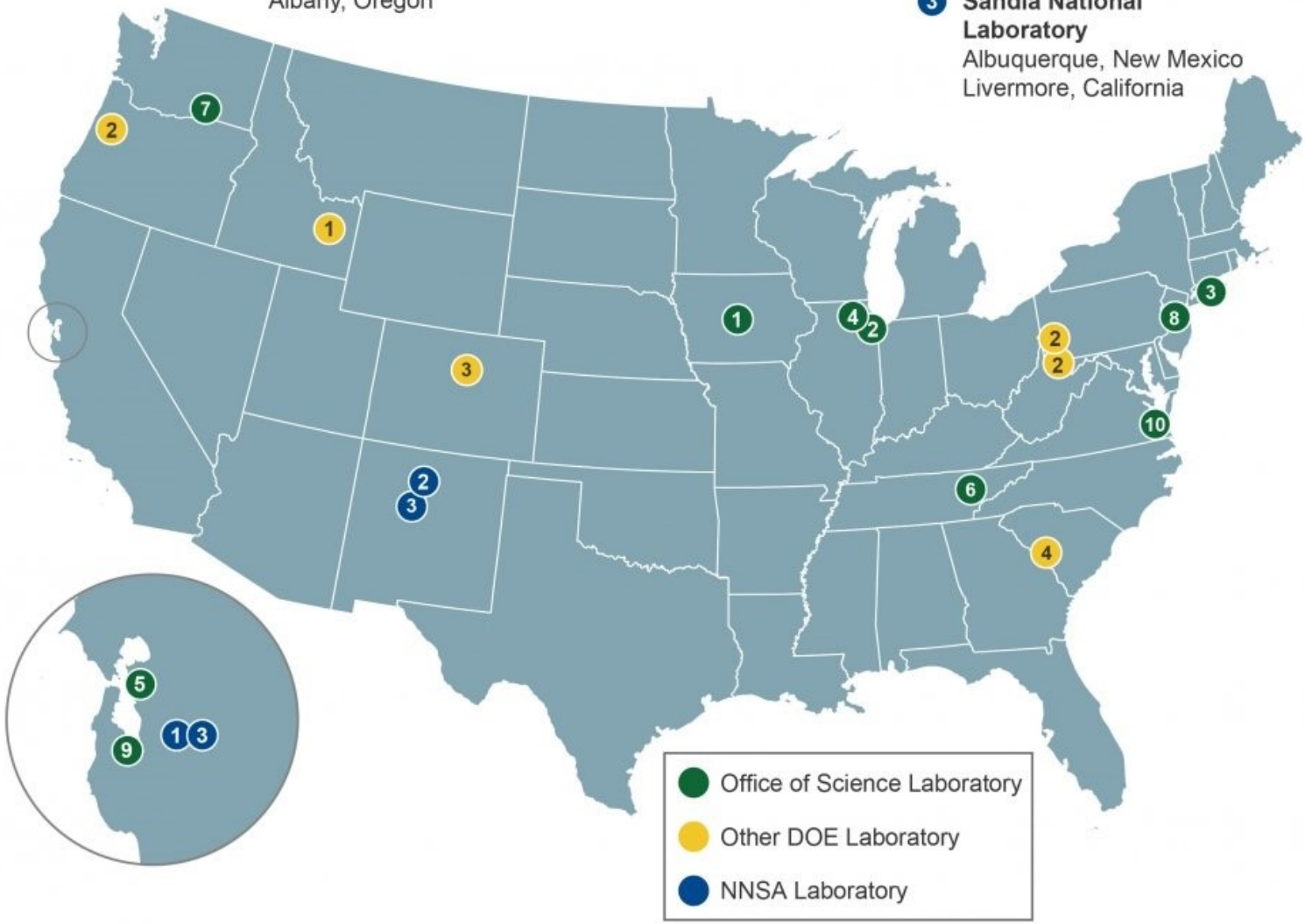
1. **Ames Laboratory**
   Ames, Iowa
2. **Argonne National Laboratory**
   Argonne, Illinois
3. **Brookhaven National Laboratory**
   Upton, New York
4. **Fermi National Accelerator Laboratory**
   Batavia, Illinois
5. **Lawrence Berkeley National Laboratory**
   Berkeley, California
6. **Oak Ridge National Laboratory**
   Oak Ridge, Tennessee
7. **Pacific Northwest National Laboratory**
   Richland, Washington
8. **Princeton Plasma Physics Laboratory**
   Princeton, New Jersey
9. **SLAC National Accelerator Laboratory**
   Menlo Park, California
10. **Thomas Jefferson National Accelerator Facility**
    Newport News, Virginia

Other DOE Laboratories

1. **Idaho National Laboratory**
   Idaho Falls, Idaho
2. **National Energy Technology Laboratory**
   Morgantown, West Virginia
   Pittsburgh, Pennsylvania
   Albany, Oregon
3. **National Renewable Energy Laboratory**
   Golden, Colorado
4. **Savannah River National Laboratory**
   Aiken, South Carolina

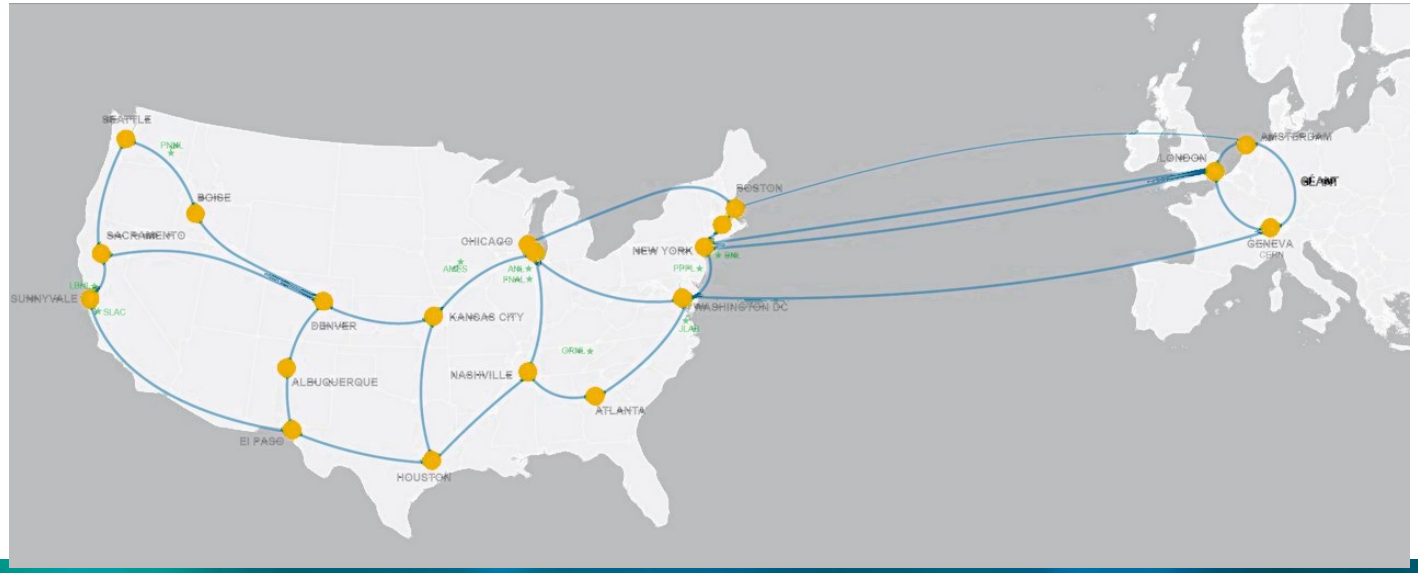
NNSA Laboratories

1. **Lawrence Livermore National Laboratory**
   Livermore, California
2. **Los Alamos National Laboratory**
   Los Alamos, New Mexico
3. **Sandia National Laboratory**
   Albuquerque, New Mexico
   Livermore, California



A Large Complex Enterprise

- **$14 Billion, 16 Major Contracts**
  - 63,380 internal users
  - 20,000 scientists & engineers
  - 53M gross square feet
  - 4,740 buildings on 1,270 sq. miles (>RI)
- **240,000 assets in 86 FISMA systems**
  - 123,000 desktops & laptops
  - 100,000 other network assets
  - 20,000 government mobile devices
- **Highly Collaborative**
  - 2,000 TB/day on ESnet
  - 50% of users are external
    - *40,000 remote only users*
    - *28,000 on-site visitor users*
  - 14,000 external co-authors

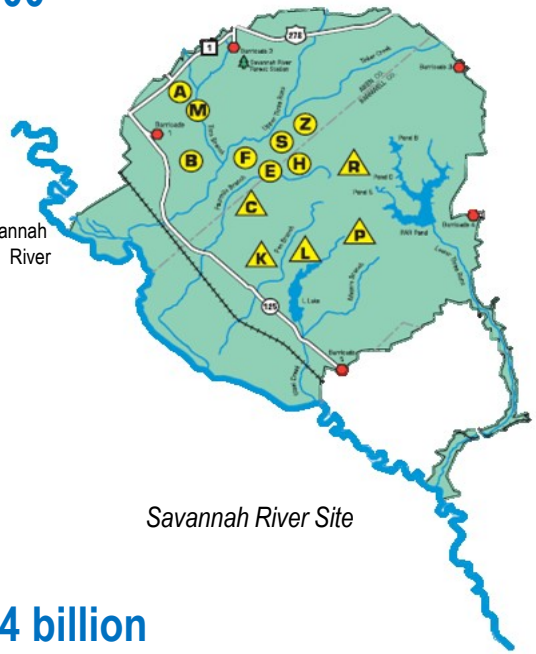


Savannah River Site at a Glance

As seen from space, SRS is an island of green in the deforested landscape.

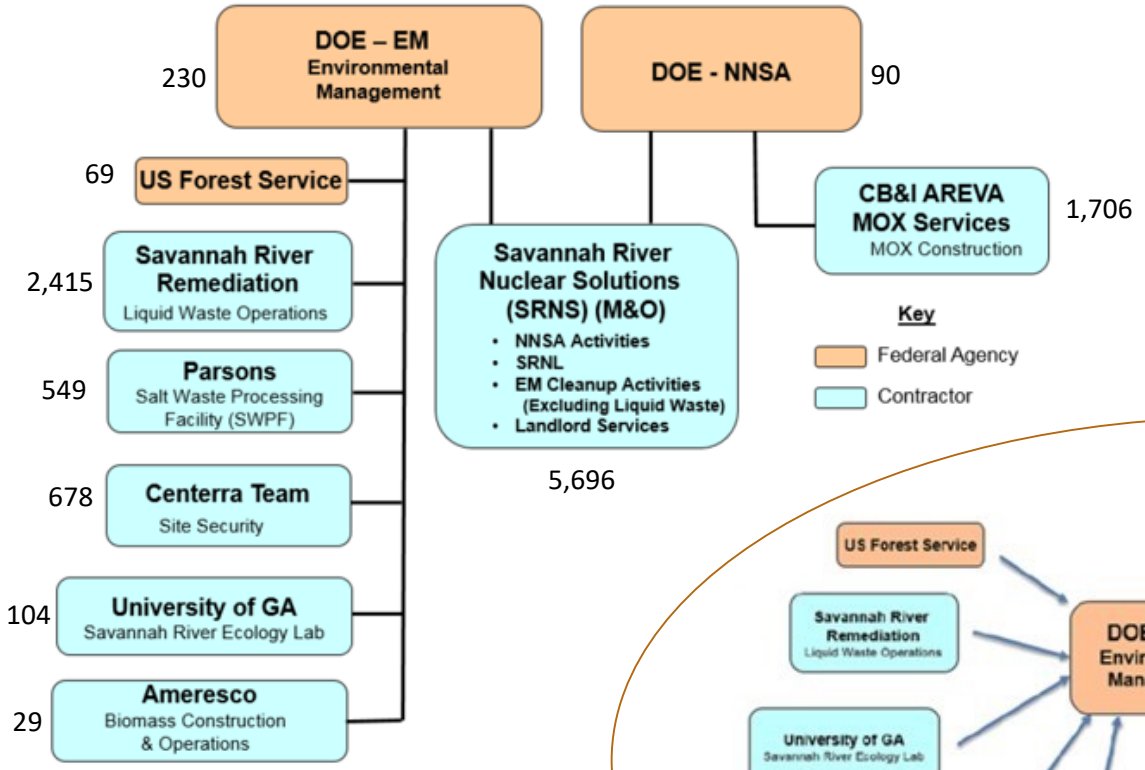
SRS is a key DOE site responsible for environmental stewardship and cleanup, waste management, and disposition of nuclear materials.

- **~803 square kilometers**
- **SRS workforce: Approximately 10,000**
  - DOE-SR and DOE-NNSA
  - **Savannah River National Laboratory**
  - **Savannah River Nuclear Solutions (M&O Contractor)**
  - Other contractors include Savannah River Remediation, Centerra SRS, CB&I AREVA MOX Services, Parsons, and the University of Georgia (Savannah River Ecology Laboratory)
- **Total Site budget approximately $2.4 billion**



Savannah River Site

SRS Workforce Structure Today



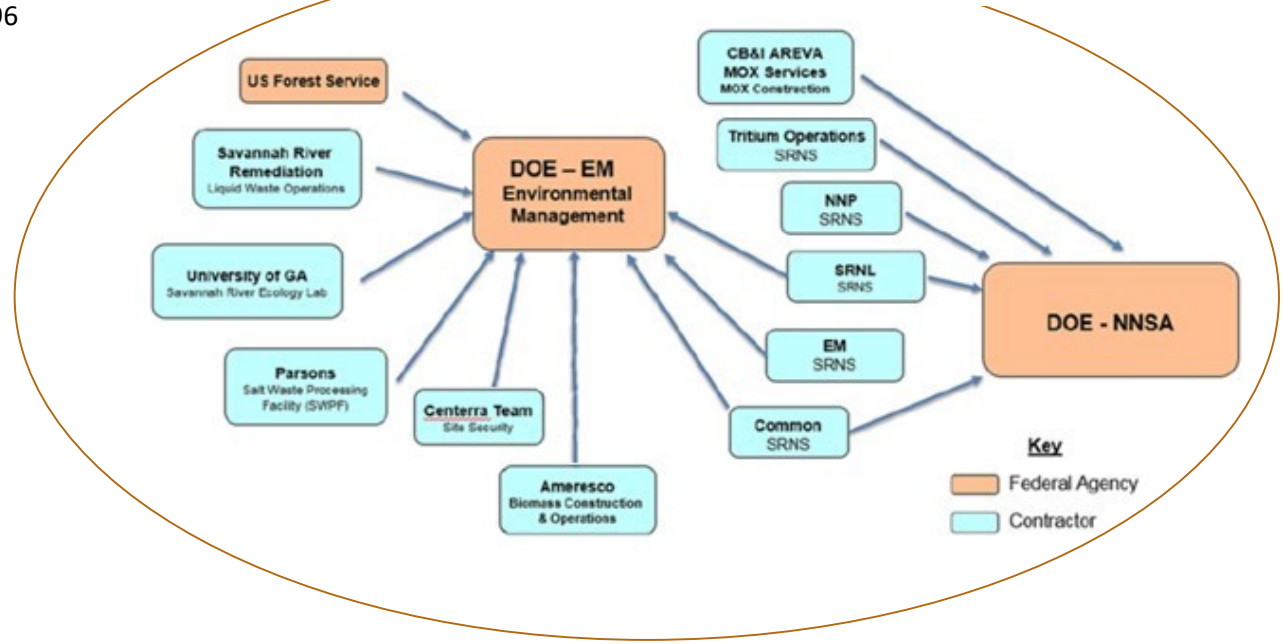
SRS Total Workforce

(incl. Permanent, Support Service, Craft, Limited Service)

≈ 11,671

(as of 9/30/18)

SRS Contractor/Department Interdependencies



We put science to work.™

Savannah River National Laboratory®

OPERATED BY SAVANNAH RIVER NUCLEAR SOLUTIONS

SRNL at a glance

Core Competencies

- Environmental Remediation & Risk Reduction
- Tritium Processing, Storage and Gas Transfer Systems
- Nuclear Materials Processing & Disposition
- Nuclear Materials Detection, Characterization & Assessment

Location | *Aiken, South Carolina*

Type | *Multidiscipline*

Founded | *1951*

Director | *Dr. Vahid Majidi*

Contractor | *Savannah River Nuclear Solutions*

Savannah River National Laboratory is a multidiscipline research and development center, where accomplished scientists and engineers solve our nation's most challenging environmental and security problems. Working with partners, we protect our nation by applying science to international security, the environment and the energy economy. We apply our unique scientific and engineering expertise to develop and deploy practical solutions with high returns on investment for our nation.

We put science to work.

923 Workforce

502 Engineers and Scientists

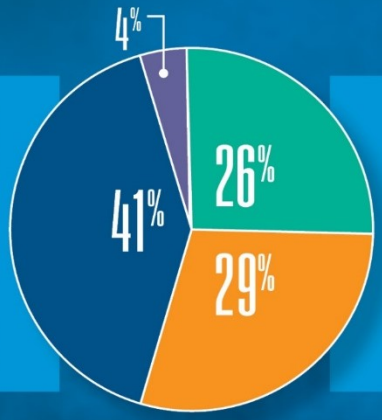
201 Ph.Ds

6 Postdoctoral Researchers

60 Graduate/Undergraduate Interns

$ 261 MILLION

FY 2019 **Overall Program Budget**



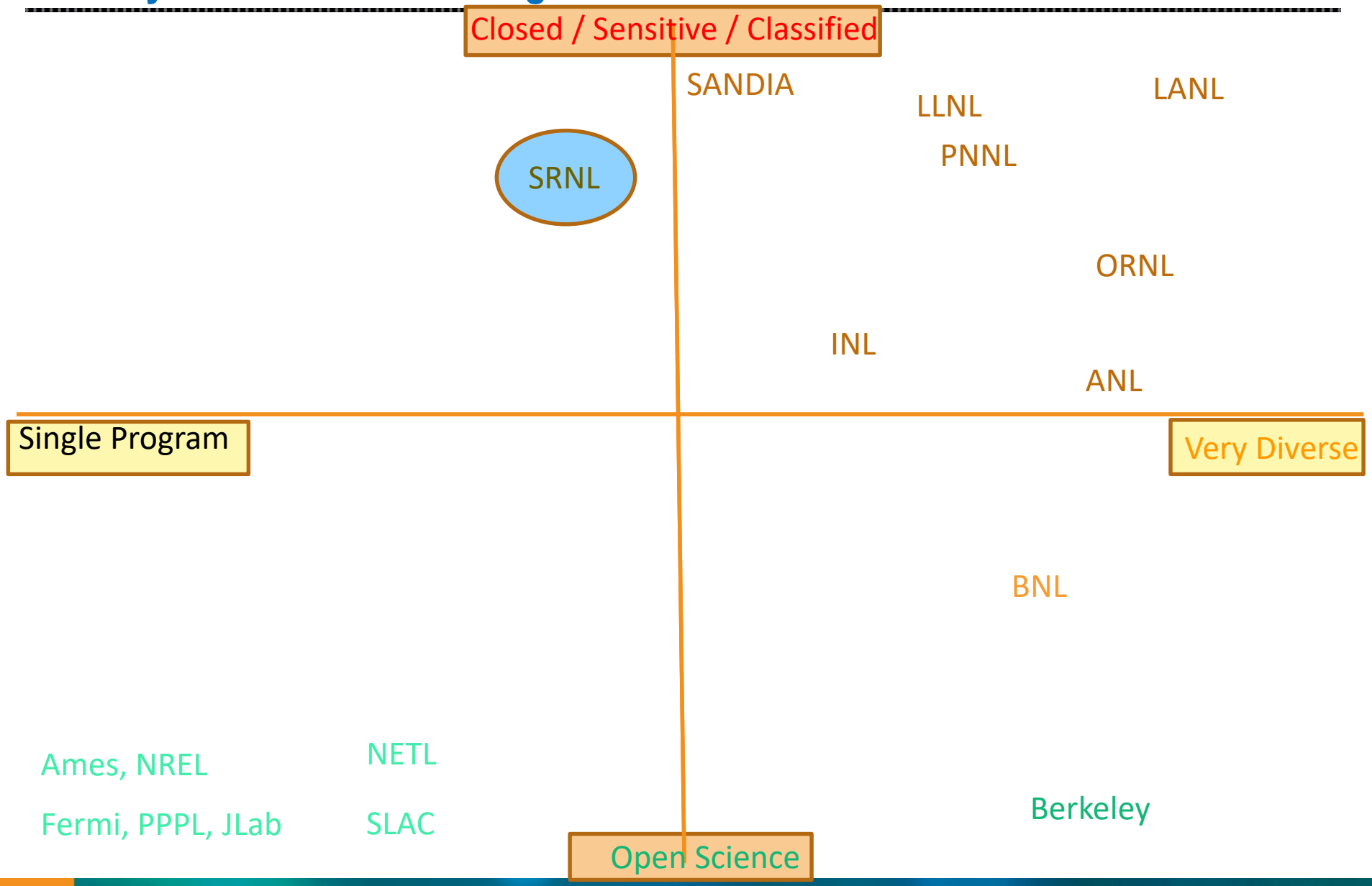
Program Areas

- Environmental Stewardship
- National Security
- Nuclear Materials Management
- Secure Energy Manufacturing

Savannah River National Laboratory

13CC00015KP FEB19

Diversity of National Lab Programs



Good Buys and Bad Guys

Threats:

- National Governments
- Terrorists (and Cyber Terrorists)
- Industrial Spies
- Organized Crime
- Activists / Hacktivists
- Personally Motivated Hackers
- Unethical Commercial Advertisers
- Disgruntled Employees
- Procedure-Breaking Employees
- Curious Employees

Partners:

- Ethics Officer
- Human Resources
- General Counsel
- Security Incident Program Manager
- Classification Office
- Information Security
- Technical Security
- Authorizing Official Designated Rep
- Management
- DOE Joint Cyber Command Center (JC3)
- US Computer Emergency Response Team
- DOE Inspector General
- Law Enforcement
- Counterintelligence
- Other “Federal Agencies”

Requirements Flow Down – Unclassified Environment

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

National Institute of Standards and Technology
U.S. Department of Commerce

Committee on National Security Systems

NIST 800-53
Security and Privacy Controls for Federal Information Systems and Organizations

NIST 800-37
Guide for Applying the Risk Management Framework to Federal Information Systems

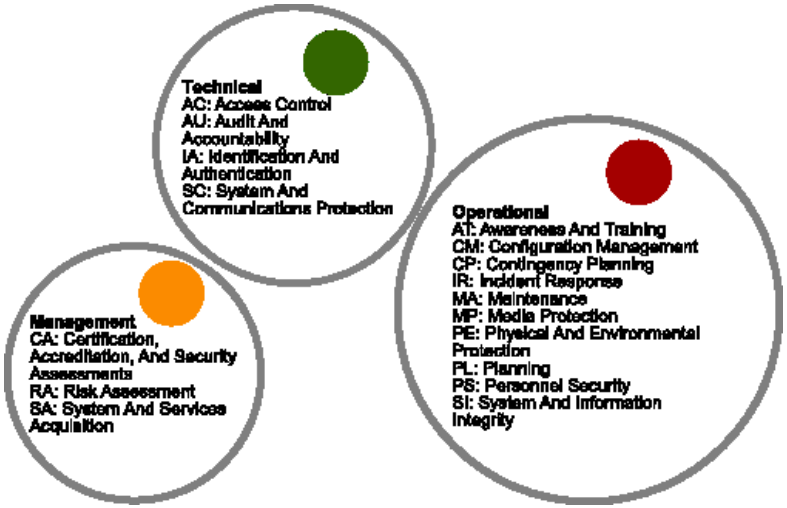
DOE O 205.1B
Cyber Security Program

DOE-EM RMAIP
Risk Management Approach Implementation Plan

SRSnet SSP
System Security Plan

SSP Exceptions

NIST Control Families



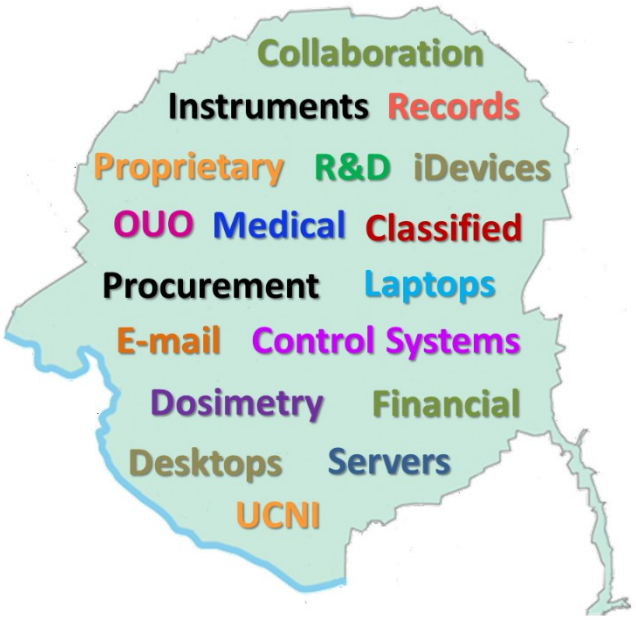
Example Cyber Security Program Elements

- **Access Controls**
  - Managing Computer Accounts – Revalidation, Cancellation
  - Identity Management / Authentication
  - Separation of Duties
  - Least Privilege Principle
  - Unsuccessful Login Attempts, Session Time Out, etc.
- **Media Management**
- **Network Segmentation**
  - Data Types
  - Classification Levels
  - Use Cases
  - Need to Know

Example Cyber Security Program Elements (cont'd)

- Employee Awareness, Training, Drills
- Configuration Management, Change Control, Maintenance, Procurement, Test and Validation.
- Audits
- Vulnerability Scanning
- Penetration Testing
- Contingency Planning / Disaster Recovery
- Incident Response
- Investigations / Forensics
- Physical Access Controls
- Cryptography
- Risk Management

Targets / Assets / Activity – (SRS Example Data)



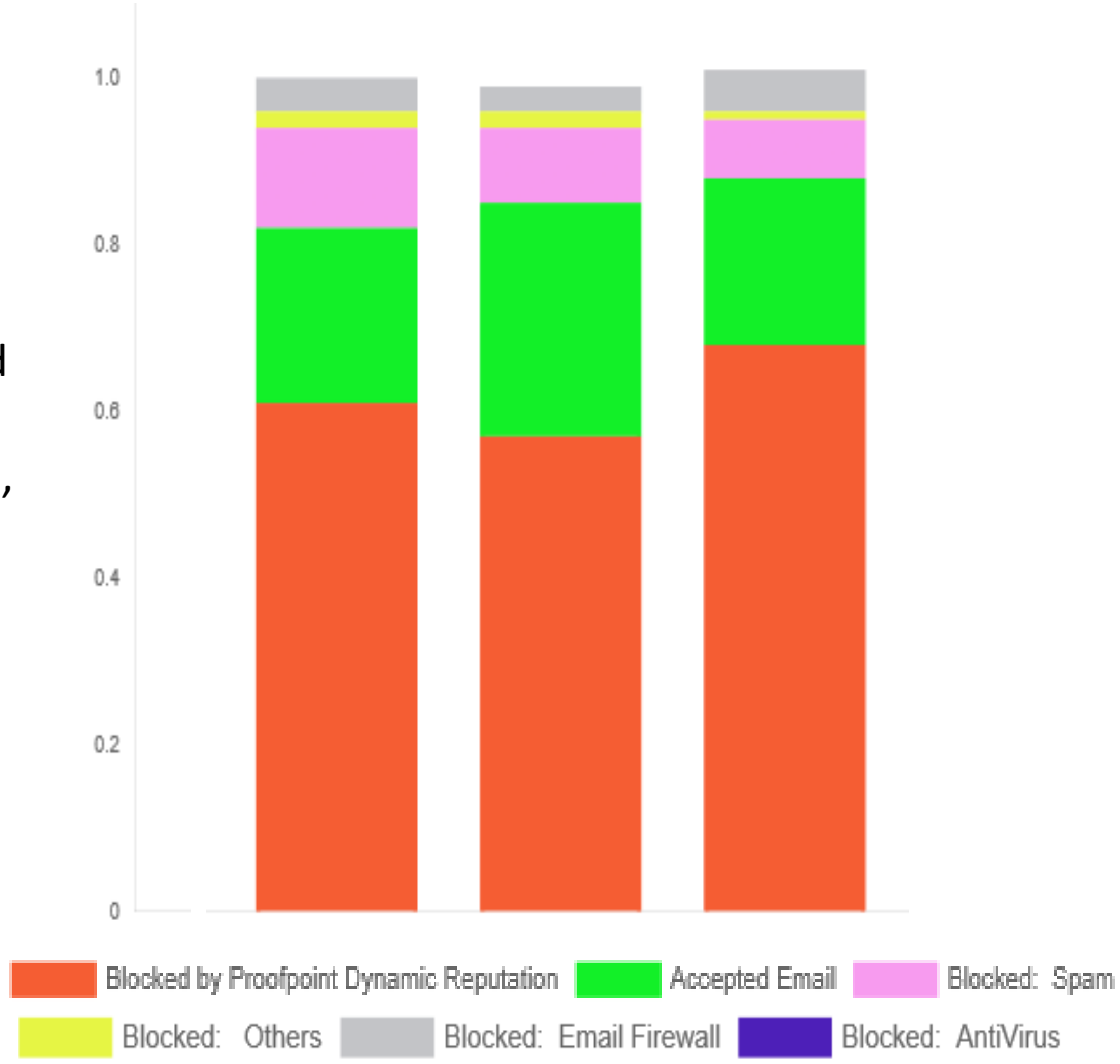
Servers 891	**Storage Area Network** >1200 TB
Networked Desktops 8370	**Incoming E-mails/month** 3,900,000
iPhones & iPads 3342	**Land Line Phones** 13,020
E-Mail Accounts 9228	**Remote Access Users** >3300
Network Switches 691	**Cell Phones** 1064

Typical Monthly Statistics

Total Log Entries / Events Processed **> 31 Billion**	Protective Action Reports Analyzed **> 200**	Average Time to Patch Vulnerabilities **< 2 weeks**
Incoming Internet Connections Blocked **> 7 Million**	Outgoing Internet Connections Blocked **> 80 Million**	Inbound Emails Blocked **> 500,000**

SRS Global Incoming Message Summary

Typical monthly statistics related to blocked mail (dynamic reputation, spam, other, firewall, and antivirus)



Security Products in Use

- **Product set is large and growing**
  - Significant learning curve for new employees
  - On-going product maintenance / operation efforts in addition to tool use
  - Devices:
    - *11 Firewalls devices*
    - *3 Web Application Firewalls*
    - *8 Proxy servers*
    - *12 IDS systems*
    - *24 Security Event (SIEM) Servers*

Cyber Security Elements

- Policy / Procedures
- Risk Assessments
- System Security Plans
- Procurement Reviews
- Cyber Exception Reviews
- Secure Configuration Baselines
- Self Assessments
- Forensics
- Anti-Phishing
- Cyber Awareness Presentations
- Media Sanitization / Disposal
- Security Incident Management
- Security Architecture
- Encryption Products
- Vulnerability Scanning
- Malware Analysis
- Log and Event Monitoring
- Perimeter Firewalls and Proxies
- Internal Firewalls
- Intrusion Detection
- Audits and Data Calls
- E-mail Scan and Filter
- DNS Security
- Anti-Virus
- Network Access Controls
- Multi-Factor Authentication
- Data Exfiltration
- Penetration Testing

What are the…

- **… biggest challenges?**
  - Complexity
    - *New technologies (Mobile, Cloud, IoT)*
    - *Sophisticated attacks evolving faster than detection technologies*
    - *Huge volume of indicators to watch*
  - Resources
    - *Recruiting, training and retraining the right people*
    - *Balance between evaluating and deploying new technologies and monitoring existing systems*
    - *Funding to stay current with growth and sophistication of the threat*
- **… biggest threats?**
  - Foreign or criminal penetration of the network
  - Attacks against infrastructure
  - Insiders
    - *Careless Insiders*
    - *Balance functionality with security*
    - *Lack of user appreciation of threat / consequences*

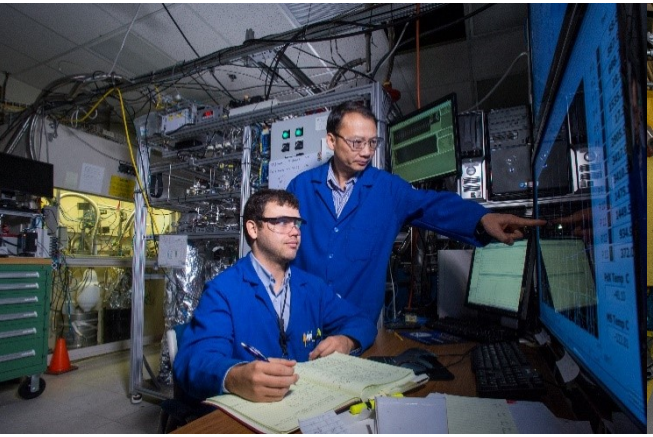
Skillsets Needed for Cyber Defense

Softer Skills

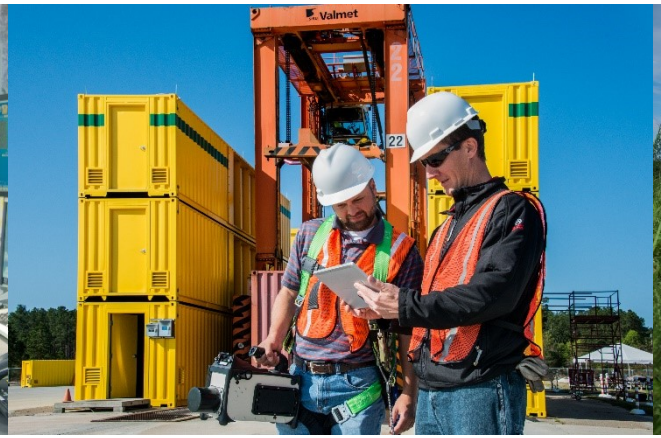
- **Analysis**
  - Risk, impact, alternatives
- **Reasonableness**
  - Security is never perfect
- **Initiative; Passion for Security**
- **Inquisitiveness; Awareness; Attention to detail**
  - Able to drill down and follow the clues
  - What does normal look like?
  - What has changed?
- **Confidentiality and Integrity**
  - Ability to hold security clearances
  - Keep “secrets” - “need to know”

Base Technical Skills

- **Networks**
- **Operating Systems**
  - Windows, Unix, Vmware
- **Firewalls**
- **Writing**
  - Precise language
  - Technical documentation
  - Targeting the right audience
- **Project Management**
- **Coding / Scripting**
  - Especially web applications
  - Regular Expressions



We protect our nation by applying science to discover practical solutions to environmental, national security, nuclear material management, and energy security challenges.

Conclusion

IT cyber protection is COMPLEX

ICS cyber is CRITICAL

Attackers are upping their game

A highly educated workforce is a MUST

Continual Learning is REQUIRED!


Supreme Air
624
KIMTECH Science
4 IN. X 250 FT.
DOUBLE SIZE ROLL
Fisherbrand
NITRILE