Putting First Things First:
Creating a Foundation for TEA Success

Susan Farrand

U.S. Department of Energy
Office of the Associate CIO for Cyber Security

Building into the Future

- The threat to information infrastructures is real.
- More complicated technology will create greater vulnerabilities.
- Awareness of the threat varies.
- Many experts expect a high impact event somewhere in the (near) future.

What we can do. . .

- Build cost-effective, graded security into every IT project from the beginning
- Focus on protecting data, not infrastructure
- Expand cyber security “best practices” to all parts of the Department
- Make cyber security a broad research priority
- Make everyone personally accountable for cyber security

It is not all about the training. . .

. . . It is all about achieving mission safely **without disruption, corruption, or loss from cyber attacks.**

People are the biggest security asset and vulnerability.

A trained workforce is a key part of defense-in-depth.

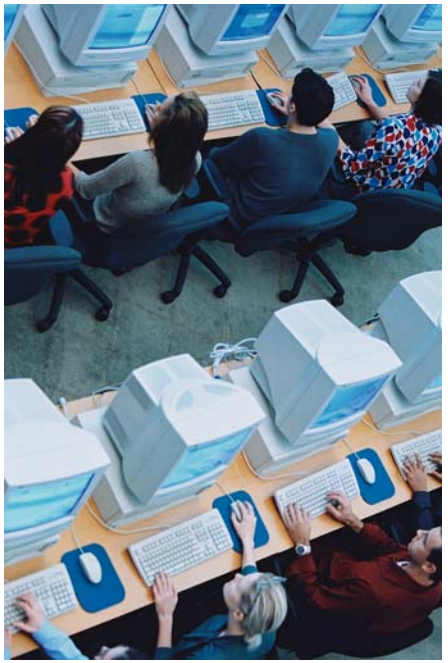
“ Go Build a Training Program”

The BIG Problem

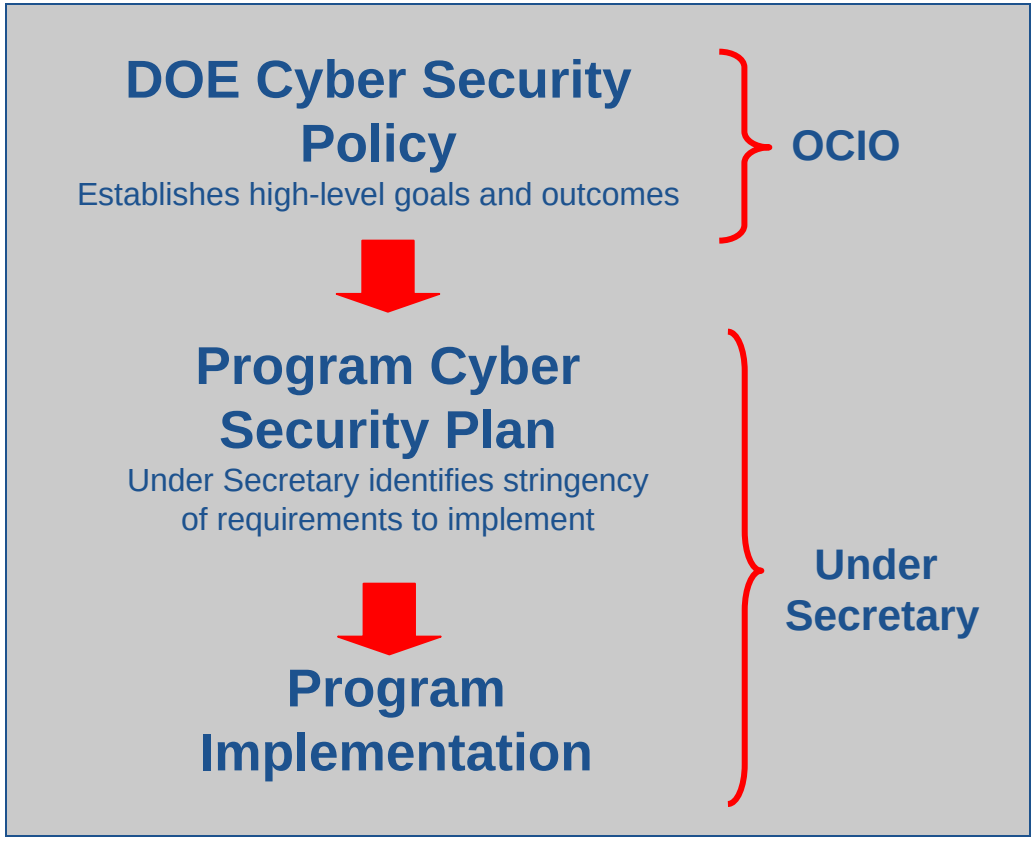
- One-size-fits-all solutions don't
  - Address needs of large or diverse organizational structures and cultures
  - Provide content and curricula tailored to functional roles and diverse missions
- Training program failure can result from
  - Incomplete assessment of organization-specific knowledge and skill requirements
  - Poor planning

Cyber Security Awareness & Training

- Why do we train?
- Who needs to be trained?
- What are the training objectives and high-level content for each audience?
- When and where should training occur?
- How should the audience be trained?
- How will training materials be developed/acquired and implemented?



Cyber Security Policy Structure



Strategic Goal

All Departmental Federal personnel and contractors are aware of and trained to execute their cyber security responsibilities and DOE requirements for protecting the confidentiality, integrity, and availability of information and information systems.

Program Objectives

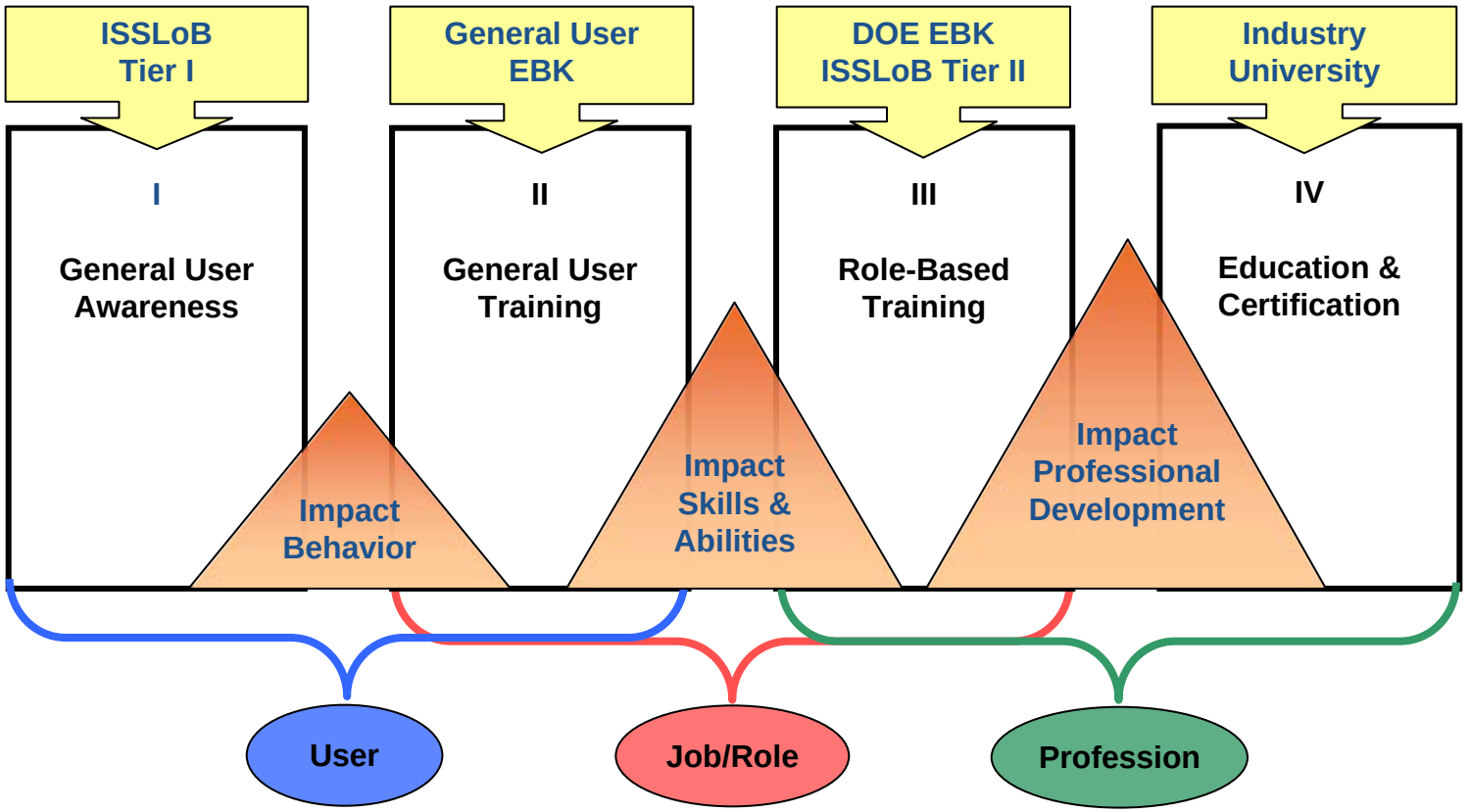
Phase 1

- Define a baseline body of knowledge,
- Define competencies, requirements, and training objectives for Department-defined functional roles, and

Phase 2

- Provide training and awareness activities and materials with emphasis on the importance of security, standards, cyber security responsibilities, and support for the competencies identified in the EBK.

Curriculum Foundation



First Steps First

1. Identify which essential functions and responsibilities for cyber security exist across the entire organization
2. Map functions and responsibilities to broad categories of roles
3. Clearly define training structure and organization-specific EBK
4. Select or develop content and role-based training plans

The EBK Advantage

- Defines minimum awareness criteria
- Assesses minimum competencies for functional roles, not job titles
- Promotes uniform competency requirements
- Provides foundational content requirements for professional development

The DOE EBK

- Two suites of competencies
  - General users
  - Functional roles with significant cyber security responsibilities
- Foundational documents
  - DHS National Cyber Security Division (NCSD) *Information Technology (IT) Security Essential Body of Knowledge (EBK)*
  - Established bodies of knowledge
  - DOE Directives and OCIO reference baselines
  - NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*

The DOE EBK (Continued)

- Thirteen competency areas
  - Defining functional statements
  - Work functions categorized as Manage, Design, Implement, or Evaluate
  - Applicable to unclassified and classified computing environments
- Foundation for functional-role curriculum
  - Curriculum development, course design, and implementation
  - Supplemental organization-specific requirements
  - Flexibility for job-responsibility competencies
- Assessment template for existing training resources (commercial and Governmental)
- Federal training and awareness requirements and professional standards

Incident Management Competency

Manage

- Coordinate with stakeholders to establish the incident management program
- Establish and coordinate activities of a CIRT to perform digital and network incident management activities
- Maintain current knowledge on network forensic tools and processes
- Establish an incident management measurement program

Design

- Develop the incident management policy, based on standards and procedures for the organization to include impact assessments and incident categorization requirements
- Create an Incident Response Management Plan in accordance with DOE policies and the PCSP
- Create incident response exercises and penetration testing activities

Implement

- Apply response actions in reaction to security incidents, in accordance with established policies, plans, and procedures to include appropriate incident characterization (i.e., Type 1 or Type 2) and categorization (i.e., low, media, high, or very high)
- Perform assessments to determine impact of loss of confidentiality, integrity, and/or availability
- Follow chain-of-custody practices in accordance with procedures set forth by the DOE CIRC

Evaluate

- Assess the efficiency and effectiveness of incident response program activities to include digital forensic investigations, and make improvement recommendations
- Examine penetration testing and vulnerability analysis results to identify risks and implement patch management
- Assess the effectiveness of communications between the CIRT and related internal and external organizations, and implement changes where appropriate

EBK Functional Role Matrix

Cyber Security EBK: A Competency and Functional Framework for Cyber Security Workforce Development	DOE Cyber Security Key Functional Roles						
	Cyber Security Program Manager (CSPM)	Designated Approving Authority (DAA)	Designated Approving Authority Representative (DAAR)	Information System Security Manager (ISSM)	Certification Agent (CA)	System Owner	Information System Security Officer (ISSO)
Data Security	M,E		E	M,D,E	I,E	D	I
Enterprise Continuity				M	E		
Incident Management	D	I		M,D			I
Cyber Security Training and Awareness	M,D,E			M,D,I,E			I
IT Systems Operations and Maintenance			E	M,D,E	E	D,I	I
Network and Telecommunications Security and Remote Access			E	M,D,E	E	D,I	I
Personnel Security				M,D		D	I
Physical and Environmental Security				M,D		D	I
Procurement						M	
Regulatory and Standards Compliance	M,D,I,E		E	M,D,I,E	I,E		I
Security Risk Management	M,D,E	E	I,E	M,D,E	I,E	D	D,I
Strategic Security Management	M,D,I,E	M		M,D,I,E			
System and Application Security		I	E	M,D,E	M,I,E	D,I	D,I

Summary for Success

- Provide cyber security training and awareness activities and materials that
  - Leverage personnel assets
  - Emphasize the importance of security, standards and personnel responsibilities
  - Reinforce protection of mission-essential data, and
  - Support the competencies identified in an organization-specific EBK

Questions?

Sue Farrand

Director, Policy, Guidance and
Planning Division
U.S. Department of Energy
Office of the Associate Chief
Information Officer for Cyber Security

202-586-2514

susan.farrand@hq.doe.gov

http://cio.energy.gov/cybersecurity/training.htm