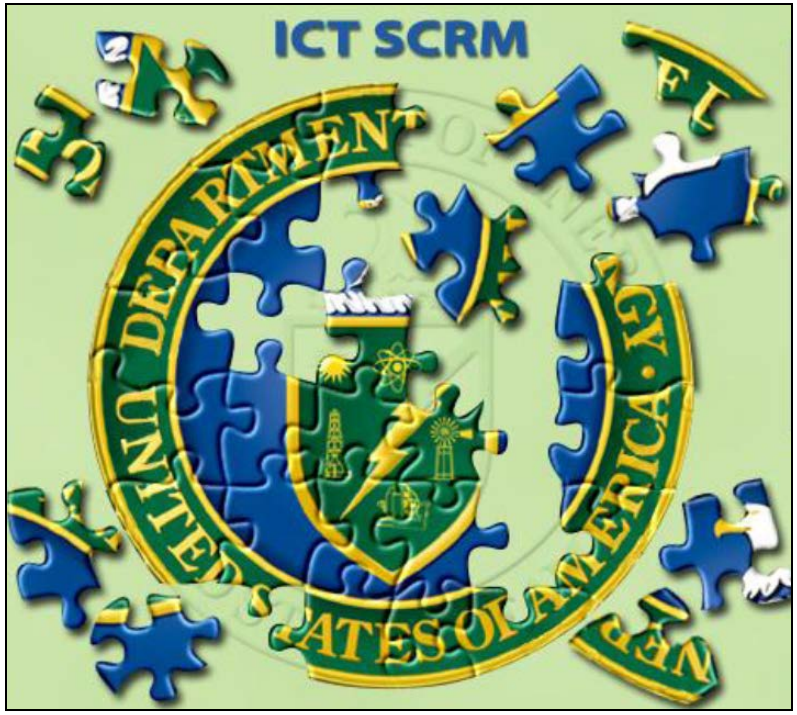
Training Module: Information Communication Technology Supply Chain Risk Management for the Information Technology Professional

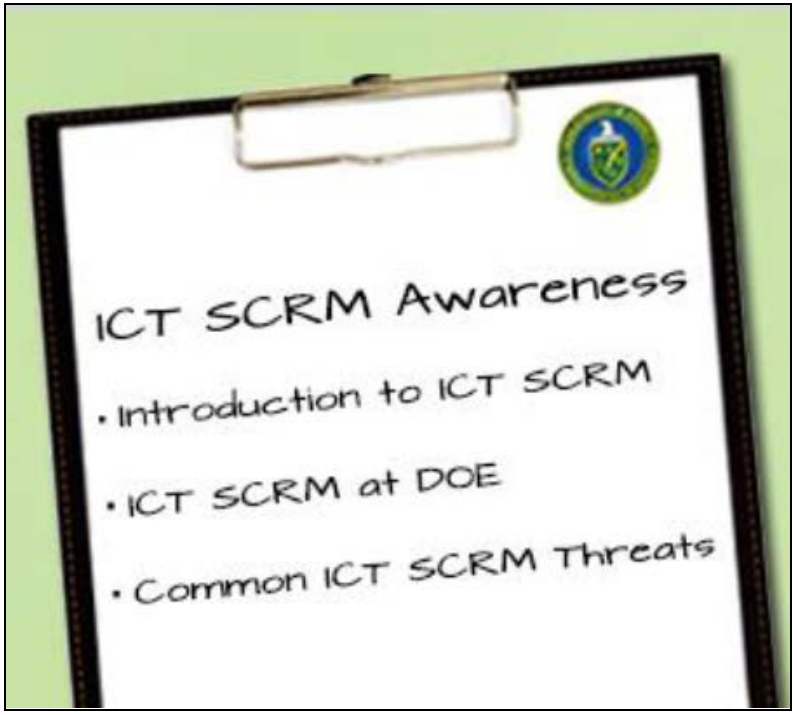
Entry for FISSEA Security Awareness, and Training Competition

Submitted by the Department of Energy
Enterprise SCRM Program

Purpose

This one-hour online course provides core competency training for Information Technology (IT) professionals regarding Information Communication Technology (ICT) Supply Chain Risk Management (SCRM).





An understanding of ICT SCRM concepts, requirements and responsibilities is essential for a consistent and comprehensive approach to protecting information assets and managing supply chain impacts to technology.

Stakeholder Buy-In

Senior management support is critical. The DOE Chief Information Security Officer introduces the course and underscores the importance of SCRM to the Department's cybersecurity program.

CIO Buy-In and support was a key driver of success. Thank You Mr. Vega!

A message from GIL VEGA, DOE's Associate CIO for Cybersecurity & Chief Information Security Officer (CISO):

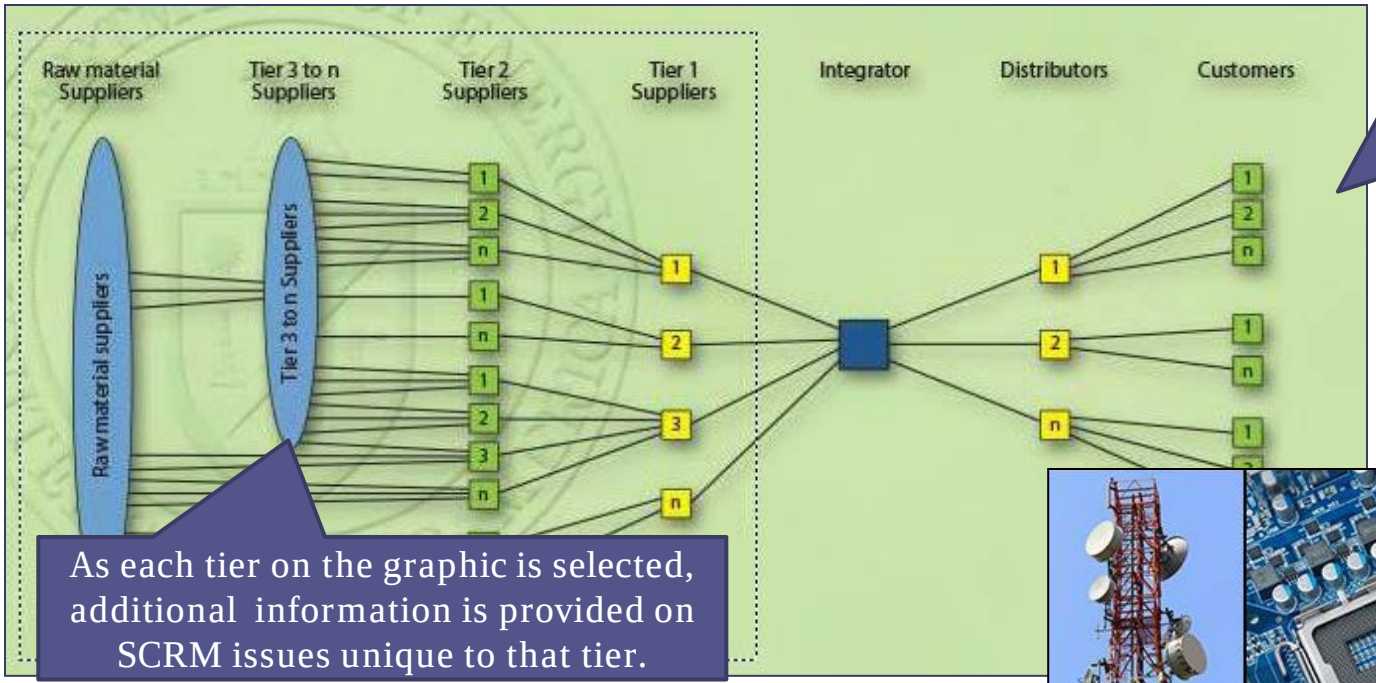
The DOE's Supply Chain Risk Management Program is an enterprise approach to managing risk and vulnerabilities associated with the acquisition, sustainment, and disposal of critical Information and Communication Technology, or ICT, components. These components store, retrieve, and transmit digital information that connects the DOE's enterprise and ensures the success of the mission. Despite ICT's benefits, increased connectivity brings increased risk of theft, fraud, and abuse. No country, industry, or Agency is immune from the inherent risks associated with global supply chains and cybersecurity. Our ability to identify and mitigate these threats is essential to achieving America's energy, environmental and nuclear challenges.

The OCIO developed this training course to further information security and cybersecurity professionals' knowledge and understanding of the ICT supply chain policies, procedures, and best practices. Additionally, this course will introduce the employee to the basic concepts of supply chain risk management, or SCRM, and its impact on the system development life cy
development and/or
Finally, this course
common ICT supply
exemplify the impor
policies and practic

The module also leveraged industry leaders, SCRM SMEs, and training professionals to ensure meaningful content and student success.

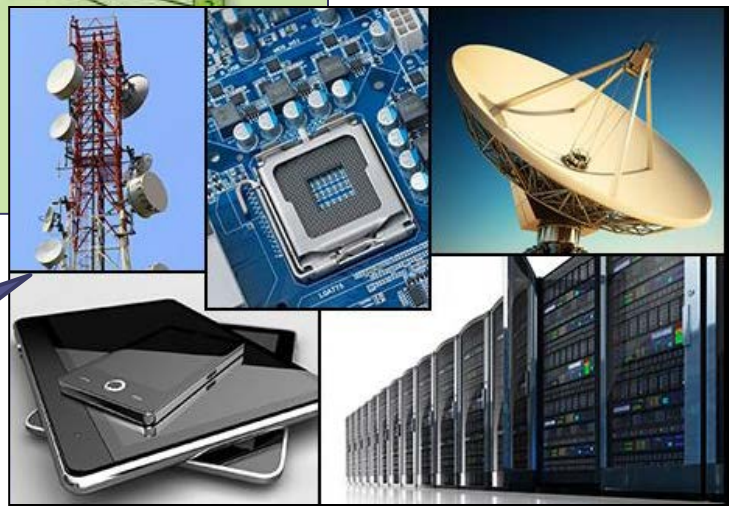
The Growing SCRM Problem

In a series of self-paced screens that incorporate text and graphics, students learn about ICT components, the growing SCRM problem, and the relationship of SCRM to cybersecurity. This format interactively reinforces foundational ICT SCRM understanding.



The module stresses the importance of managing supply chain risk introduced through global production and distribution of ICT components.

As each tier on the graphic is selected, additional information is provided on SCRM issues unique to that tier.



It also discusses how growing dependence on ICT components exacerbates the SCRM problem!

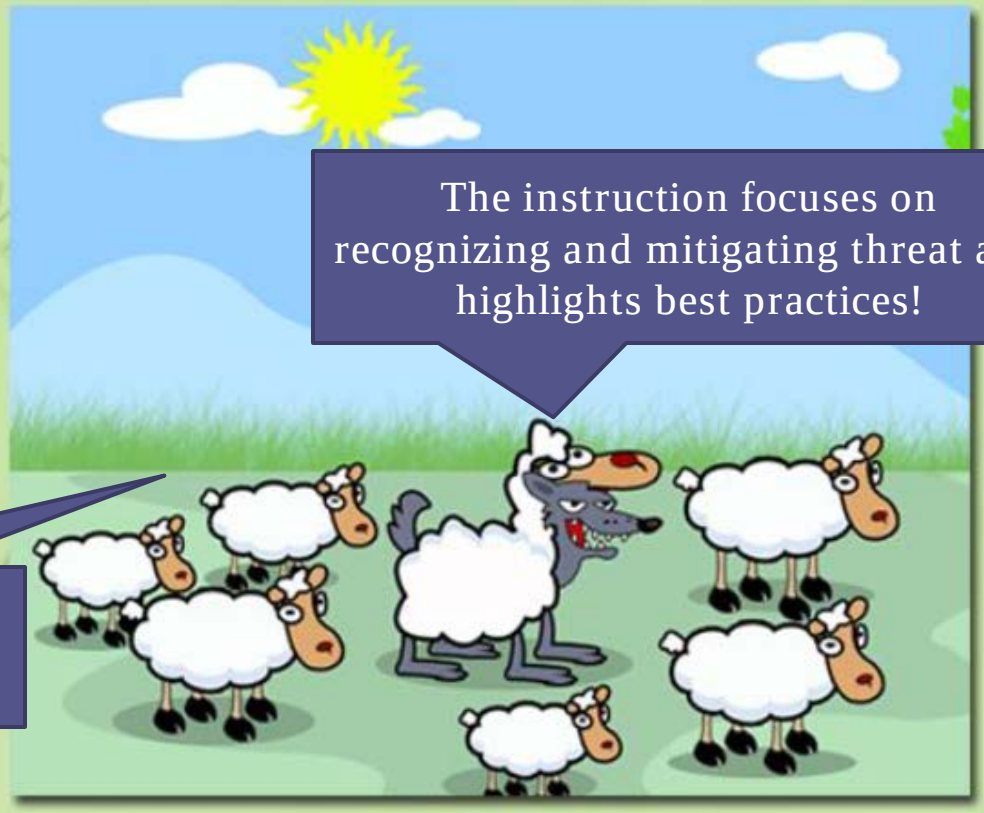
Unseen Threats: The ICT SCRM Challenge

The module details supply chain risk threat vectors, both seen and unseen. Educating students about the myriad of supply chain risks is essential to addressing the problem from a holistic perspective.

The Unseen Threat

ICT SCRM primarily involves five different challenges:

- Installation of malicious logic in hardware or software
- Installation of counterfeit hardware or software
- Failure or disruption in the production or distribution of a critical product or service
- Reliance upon a malicious or unqualified supplier
- Installation of unintentional vulnerabilities



The instruction focuses on recognizing and mitigating threat and highlights best practices!

Insider threats are both intentional and unintentional!

ICT SCRM Policy, Procedures, & Guidance

Instruction includes discussion of documents that direct, support, and guide programmatic organizations through the development, implementation, and sustainment of SCRM processes.

The following documents are **Key Drivers** of ICT SCRM policy and procedures:

- **Committee on National Security Systems (CNSS) Directive 505**, *(U) Supply Chain Risk Management (SCRM)*
- **National Institute of Standards and Technology (NIST) IR 7622**, *Notional Supply Chain Risk Management Practices for Federal Information Systems*, October 2012
- **NIST Special Publication (SP) 800-53, Rev 4**, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013
- **NIST SP 800-53A, Rev 1**, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, June 2012
- **NIST Federal Information Processing Standards (FIPS) Publication 199**, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- **NIST FIPS Publication 200**, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- **DOE O 205.1B**, Change 2, Department of Energy Cyber Security Program, 5-16-2011

Content of this course is also based on all these documents.

DOE internal policy developed by the Enterprise SCRM Program.

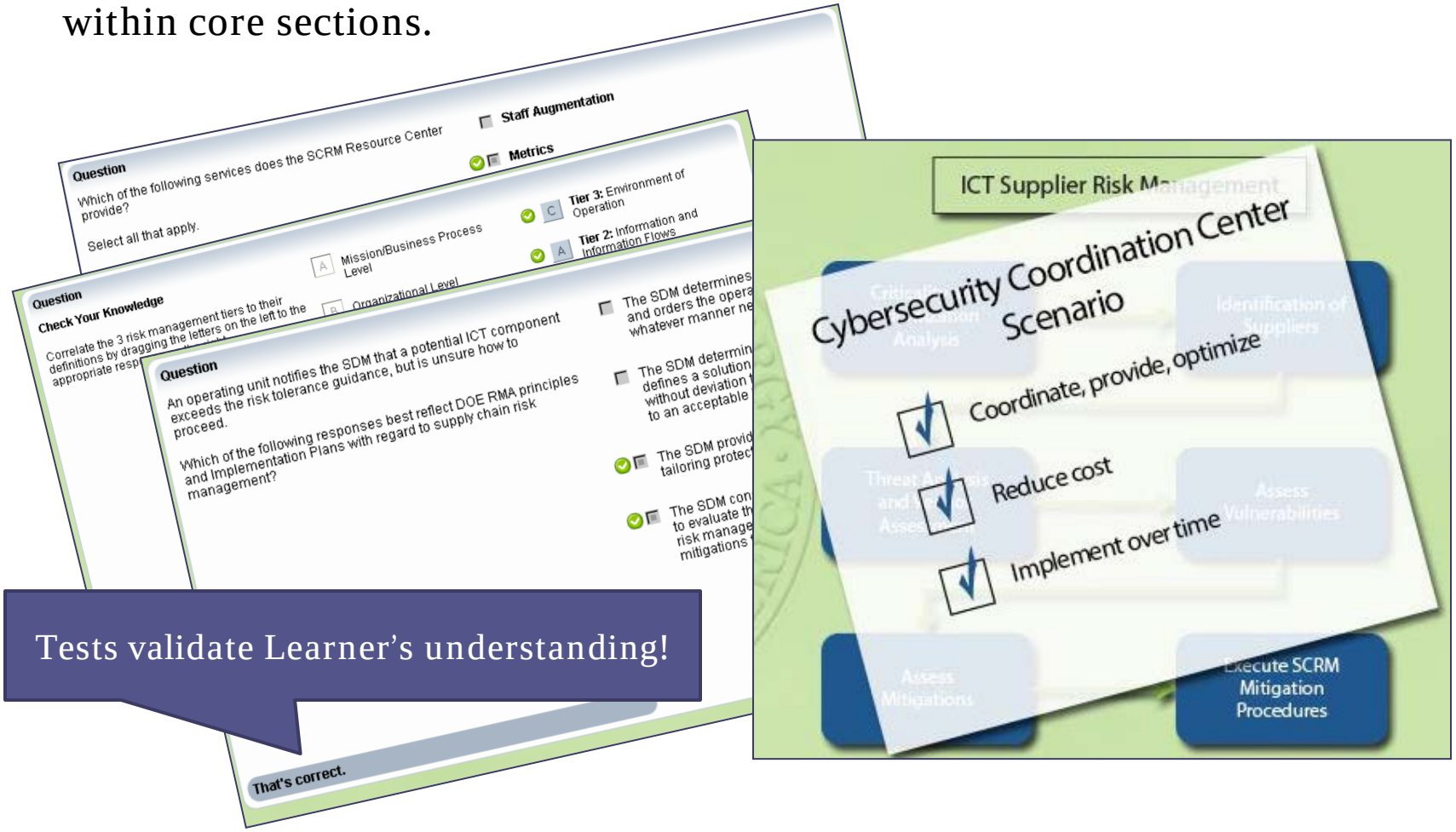
DOE's Approach to Supply Chain Mitigation

Students are introduced to best practices as well as their specific roles in addressing SCRM issues. Students interactively experience each step of the DOE Six Step SCRM Process.

The IT professional's roles and responsibilities are identified as the student selects each step!

Testing and Learning Validation

Pre-tests assess the readiness of the student for the module and post-tests evaluate knowledge retention and understanding at the end of each section of the module. Interim reinforcement of concepts also occurs intermittently within core sections.



Tests validate Learner's understanding!

Training Scenarios/Vignettes

A unique feature of the module enumerates real world threat scenarios and involves students in the process of identifying threats and vulnerabilities, assessing their impact, and implementing mitigation procedures. Presented at the end of the course, this activity ties together core SCRM competencies in a meaningful, relatable way.

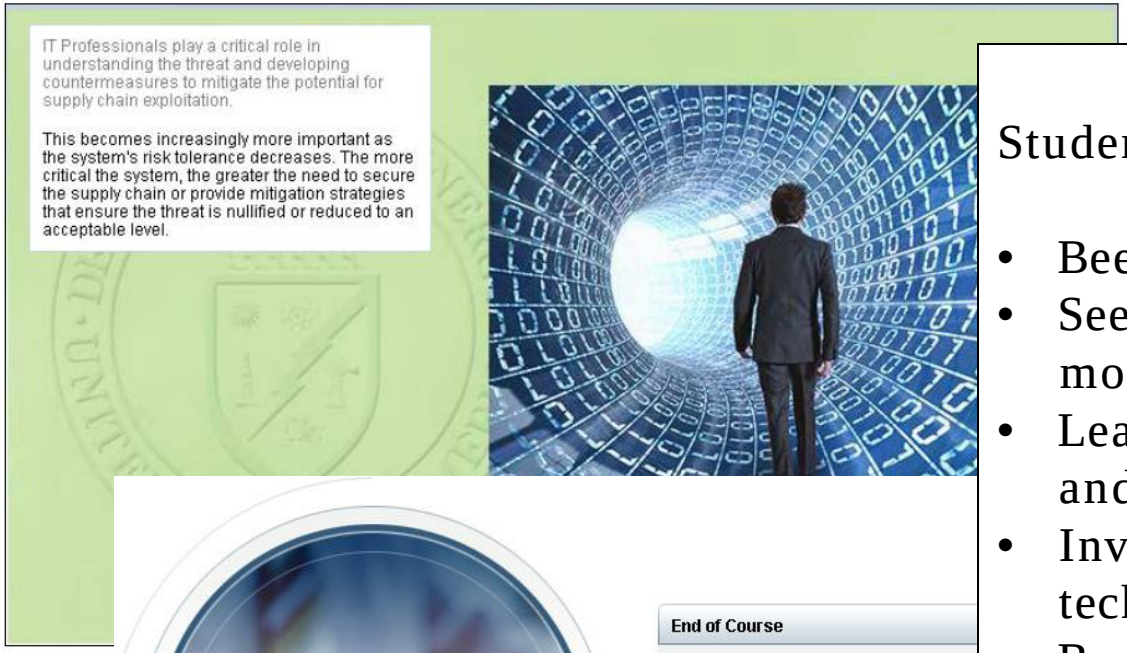
Identifying lessons learned after each scenario reinforces the module's core content!

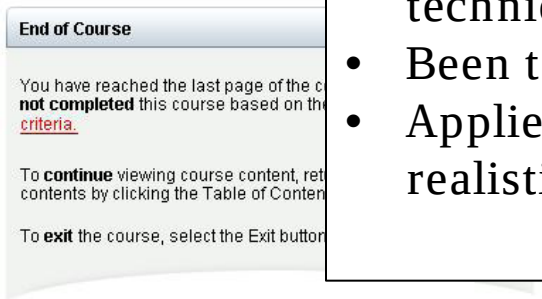
Lessons Learned

This scenario demonstrates the need for a supply chain risk management program that provides a robust trusted relationship between Government Agencies and well-vetted and trusted vendors. Identification of potential vendors, and a robust threat analysis would have assisted in the development of specific procurement language and countermeasures.

How could the Government Agency in this case have secured the supply chain and prevented the incident?

Training Take-Aways





Students have –

- Been instructed in their roles
- Seen the DOE SCRM process model
- Learned about the supply chain and its risks to ICT
- Investigated mitigation techniques
- Been tested for understanding
- Applied their understanding to realistic examples