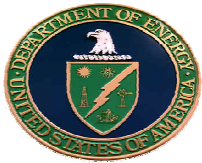




*Training...Knowledge...Competency...Success*





U.S. Department of Energy  
Office of the Associate CIO


## Course Catalogue

Training resources available from  
IM-31, Policy, Guidance, and Planning Division or  
DOE Online Learning Center2 (OLC2)  
<https://olc2.energy.gov/plateau/user/login.jsp>


The following courses have been identified as training resources that either provide general cyber security awareness material or have been selected to satisfy cyber security training and awareness requirements for general users and for personnel with job responsibilities identified as *key cyber security functional roles*. These roles include Cyber Security Program Manager (CSPM), Designated Approval Authority or Representative (DAA/DAAR), Information Systems Security Manager (ISSM), Certification Agent (CA), Information System Security Officer (ISSO), and System Owner. Any questions regarding this catalogue can be directed to Sue Farrand, Director, IM-31 Policy, Guidance, and Planning, Division at [susan.farrand@hq.doe.gov](mailto:susan.farrand@hq.doe.gov) or 202-586-2514.

### General Cyber Security Awareness


Title	Transmission Medium	Description	Course Number	Date
Information Technology (IT) Security Basics & Literacy		This course introduces several cyber security foundational topics such as threats and vulnerabilities; malicious code; principles of confidentiality, integrity, and availability; General Support Systems (GSS); Major Applications (MAs); critical infrastructure protection; disaster recovery and business resumption plans; privacy act; etc.	49930i	3/08/07
Information Security Awareness		This course focuses on managing cyber threats and vulnerabilities. Examples of attacks are given to include passive, active, malicious and non-malicious insider, etc. This class also addresses risks associated with remote users.	#fgov_01_a12_1e_enu	6/03/08


Title	Transmission Medium	Description	Course Number	Date
Operations Security (OPSEC)		This instructor-led course focuses on resources, policies, and training that deny unauthorized individuals or groups access to classified and sensitive-unclassified information. Emphasis is placed on the exploitable sources of information normally available to an adversary and on cost-effective countermeasures to deny or delay the availability of such information. The course requires a minimum score of 80% based on administered testing results and completion of a 10-hour practical exercise. <i>Note: This course is offered at the DOE National Training Center (NTC). Prerequisites for this course include ISC-141DE, OPSEC Overview. For more information contact <a href="mailto:djeffers@ntc.doe.gov">djeffers@ntc.doe.gov</a>.</i>	ISC-241	6/17/05

### Annual Cyber Security Refresher Briefing






Title	Transmission Medium	Description	Course Number	Date
Information Systems Security Awareness		This course is required to be successfully completed by all DOE employees annually. The course address major security disciplines to include technical, logical, physical, operational, and personnel security as well as describes DOE-specific cyber security requirements. This course is ISSLoB compliant.	Federal_ISS	6/08


### Designated Approving Authority

Title	Transmission Medium	Description	Course Number	Date
Information Security & Risk Management		This course is required to be successfully completed by all individuals appointed as a Designated Approval Authority (DAA) or a Designated Approval Authority Representative (DAAR) within 6 months of his/her appointment. The course addresses risk management principles to include risk categories, security planning, threat analysis, vulnerability and asset evaluation, and risk	243962	7/27/07

Title	Transmission Medium	Description	Course Number	Date
		analysis, evaluation, and mitigation.		
<b>Security Architecture &amp; Design</b>		<p>This course is required to be successfully completed by all individuals appointed as a Designated Approval Authority (DAA) or a Designated Approval Authority Representative (DAAR) within 6 months of his/her appointment. This course addresses the Certification &amp; Accreditation (C&amp;A) Security Evaluation Process as well as the common principles behind computer architectures and security models. The course utilizes CISSP language.</p>	243975	7/27/07

## Master Listing (Alphabetical Order)

Title	Transmission Medium	Description	Course Number	Date
Information Security Awareness		This course focuses on managing cyber threats and vulnerabilities. Examples of attacks are given to include passive, active, malicious and non-malicious insider, etc. This class also addresses risks associated with remote users.	#fgov_01_a12_1e_enus	6/03/08
Information Security & Risk Management		This course is required to be successfully completed by all individuals appointed as a Designated Approval Authority (DAA) or a Designated Approval Authority Representative (DAAR) within 6 months of his/her appointment. The course addresses risk management principles to include risk categories, security planning, threat analysis, vulnerability and asset evaluation, and risk analysis, evaluation, and mitigation.	243962	7/27/07
Information Systems Security Awareness		This course is required to be successfully completed by all DOE employees annually. The course address major security disciplines to include technical, logical, physical, operational, and personnel security as well as describes DOE-specific cyber security requirements. This course is ISSLoB compliant.	Federal_ISS	6/08
Information Technology (IT) Security Basics & Literacy		This course introduces several cyber security foundational topics such as threats and vulnerabilities; malicious code; principles of confidentiality, integrity, and availability; General Support Systems (GSS); Major Applications (MAs); critical infrastructure protection; disaster recovery and business resumption plans; privacy act; etc.	49930i	3/08/07
Operations Security (OPSEC)		This instructor-led course focuses on resources, policies, and training that deny unauthorized individuals or groups access to classified and sensitive-unclassified information. Emphasis is placed on the exploitable sources of information normally available to an adversary and on cost-effective countermeasures to deny or delay the availability of such information. The course requires a minimum score of 80% based on administered testing results and completion of a 10-hour practical exercise.	ISC-241	6/17/05

Title	Transmission Medium	Description	Course Number	Date
		<p><i>Note: This course is offered at the DOE National Training Center (NTC). Prerequisites for this course include ISC-141DE, OPSEC Overview. For more information contact <a href="mailto:djeffers@ntc.doe.gov">djeffers@ntc.doe.gov</a>.</i></p>		
<b>Security Architecture &amp; Design</b>		<p>This course is required to be successfully completed by all individuals appointed as a Designated Approval Authority (DAA) or a Designated Approval Authority Representative (DAAR) within 6 months of his/her appointment. This course addresses the Certification &amp; Accreditation (C&amp;A) Security Evaluation Process as well as the common principles behind computer architectures and security models. The course utilizes CISSP language.</p>	243975	7/27/07