

## Introduction to the Table of Cyber Security Competencies

The [Table of Competencies](#), Chart 3, comprises the core body of knowledge (CBK) of the cyber security profession. The purpose of these competencies is to translate the theoretical knowledge needed into specific job competencies. These fundamental concepts have been taken from the documents in which they are defined: the NIST SP 800-16, the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4011, *National Training Standard for Information Systems Security (INFOSEC) Professionals*, and Department of Energy position descriptions.

The topics of study and knowledge comprising the cyber security CBK are listed in Chart 1 below. These topics represent the theoretical knowledge needed.

<b>Chart 1 Cyber Security Core Body of Knowledge</b>		
<ul style="list-style-type: none"><li>• Laws and regulations</li><li>• IT security program</li><li>• System environment</li><li>• System interconnection</li><li>• Information sharing</li></ul>	<ul style="list-style-type: none"><li>• Life Cycle controls</li><li>• Management controls</li><li>• Operational controls</li><li>• Technical controls</li></ul>	<ul style="list-style-type: none"><li>• Roles and responsibilities</li><li>• Awareness, training, and education</li><li>• Handling sensitive and classified information</li></ul>

The above topics are not easily translated into job duties or performance. Therefore, the following DOE-specific categories listed in Chart 2 were created to classify the day-to-day activities of a cyber security professional. The categories have been organized within a framework of the systems life cycle.

In the competency chart, Chart 3, individual skills related to the cyber security CBK are listed under the corresponding category. This coordination provides the link that allows the theoretical knowledge to be translated into job duties, while also providing a clear link to the DOE workplace.

<b>Chart 2 DOE Categories</b>
<ul style="list-style-type: none"><li>• Laws regulations and policies</li><li>• Security program management</li><li>• Design of Security Systems, Processes and Procedures</li><li>• Development of Security System Processes and Procedures</li><li>• Operation of Security Systems</li><li>• Audit Management</li><li>• Test and Evaluate Security Systems and Procedures</li><li>• Terminate Security Systems</li></ul>

Congress initially asked DOE to ensure training was provided for five groups of employees. However, the Subject Matter Experts in the Policy Working Group have defined seven groups of jobs, or audiences, that require the competencies. The groups include:

- Senior Managers
- Line Managers
- IT Professionals
- IT Managers
- System Administrators
- System Managers
- Users

For these groups the competencies are broken into three levels of skills required in their jobs: beginning, intermediate or advanced.

Using these competencies, DOE managers can:

- Identify activities done by positions in the group or audience, and then by the level in the group
- Write performance elements for competencies at an appropriate level
- Identify training needs and the comparative level of instruction (beginning, intermediate and advanced)
- Develop Individual Training Plans (ITPs) and Individual Development Plans (IDPs) for staff members.

Using the competencies managers can easily define the roles of a job in one of these groups, and determine the types of activities and training needs that are associated with each level of expertise.

In order to ensure that this information is directly applicable to the DOE workforce, a panel of Subject Matter Experts validated the chart. Members of the DOE Cyber Security Policy Working Group (PWG) reviewed and revised the competencies when the group met in January 2001, providing feedback on the levels of experience required for each competency.