All links below take you to the datasheet for that KU.

Core 2Y Knowledge Units

Basic Data Analysis
Basic Scripting
Cyber Defense
Cyber Threats
Fundamental Security Design Principles
Information Assurance Fundamentals
Introduction to Cryptography
Information Technology System Components
Networking Concepts
Policy. Legal, Ethics and Compliance
Systems Administration

NSA/DHS CAE-IA/CD Knowledge Units - Core 2Y

			Courses	CIS 146	CIS 214	CIS 245	CIS 246	CIS 280
Click here to return to KU Listing				(Click Here) READ THIS FIRST: This matrix is for the				
Basic Data Analysis								
Provide students with basic abilities to manipulate data into meaningful information.								
	Topics							
		Summary statistics		IX a-h				
		Graphing/Charts		XI a-h				
		Spreadsheet Functions		IX a-h				
		Problem Solving		X c	IIc,IV,V,VI,IX	VI, VII	II, III,Vf,Vo	V c.
	Outcomes							
	Students will be able to:							
		Apply standard statistical inference procedures to draw conclusions from data		IX a-h	IIc,IV,V,VI,IX	VI, VII	II, III,Vf,Vo	V c.

NSA/DHS CAE-IA/CD Knowledge Units - Core 2Y

		Courses	CIS 146	CIS 214	CIS 245	CIS 246	CIS 280						
Click here to return to KU Listing				(Click Here) READ THIS FIRST: This									
Basic Scripting													
Provide students with the ability to create simple scripts/programs to automate and perform simple operations. This knowledge should include basic security practices in developing scripts/programs (e.g., bounds checking, input validation).													
	Topics												
		*Basic Security											
		Bounds checking, input validation			VII								
		Program Commands			VII								
		Program Control Structures			VII								
		Variable Declaration			VII								
		Debugging			VII								
		Scripting Language (e.g. PERL, Python, BASH, VB Scripting, Powershell)		IIIk.l., IV	VII								
		*Basic Boolean logic/operations											
		AND / OR / XOR / NOT	XIII		VII								
	Outcomes												
	Students will be able to:												
		Demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks)	XIII		VII								
		Write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL)			VII								
		Write simple linear and looping scripts			VII								

NSA/DHS CAE-IA/CD Knowledge Units - Core 2Y

Courses	CIS 146	CIS 214	CIS 245	CIS 246	CIS 280						
Click here to return to KU Listing		(Click Here) READ THIS FIRST: This matrix is for the									
Cyber Defense											
Provide students with a basic awareness of the options available to mitigate threats within a system.											
Topics											
Network mapping (enumeration and identification of network components)			V, VI	I,III,IV	II.d.						
*Network security techniques and components											
Access controls, flow control, cryptography, firewalls, intrusion detection			V, VI,XII, XIII		VI.h, VIII						
Applications of Cryptography		IX	XII, c, d, h		VIII.b.						
Malicious activity detection / forms of attack			III	V, VI	VII.i						
Appropriate Countermeasures		III.j	XIII	II.i, V.q, IV.l.q	VII.f.						
Trust relationships					VII.g.						
*Defense in Depth											
Layering of security mechanisms to achieve desired security			XIII	I.g.iii	IV.g.						
*Patching											
OS and Application Updates	V.f.	II.h,.v,V	VII.o		V.c.						
Vulnerability Scanning		II.d.iv	VIII.l	III.m.i,ii.	VII.l.						
Vulnerability Windows (0-day to patch availability)		II.h,.v,V	VII.l,m								
Outcomes											
Students will be able to:											
Describe potential system attacks and the actors that might perform them			III	V, VI	VII.i						
Describe cyber defense tools, methods and components	V.f.		V, VI,XII, XIII		VI.h, VIII						
Apply cyber defense methods to prepare a system to repel attacks			III	V, VI	VII.i						
Describe appropriate measures to be taken should a system compromise occur		III.j	XIII	II.i, V.q, IV.l.q VIII.d.i	VII.f.						

NSA/DHS CAE-IA/CD Knowledge Units - Core 2Y

Courses	CIS 146	CIS 214	CIS 245	CIS 246	CIS 280						
Click here to return to KU Listing		(Click Here) READ THIS FIRST: This matrix is									
Cyber Threats Provide students with basic information about the threats that may be present in the cyber realm.											
Topics											
Adversaries and targets	V.a		III	I.b,i	II.c,d.						
Motivations and Techniques	V.d		I.b.	I.b,i	II.a.						
The Adversary Model (resources, capabilities, intent, motivation, risk aversion,				I.b,i	V						
*Types of Attacks											
Password guessing / cracking		II.c	III.j., XII.r.	V	II.c.						
Backdoors / trojans / viruses / wireless attacks		V.h	III.e.	VI.f	II.c.						
Sniffing / spoofing / session hijacking		I	III.o.	VII	II.c.						
Denial of service / distributed DOS / BOTs		VII.f,iii	III.l.	IX	II.c.						
MAC spoofing / web app attacks / 0-day exploits		III.j,iii	X.g.	VII.e	II.c.						
Vulnerabilities that enable them		IV.d	X.e.	VII	II.c.						
Attack Timing (within x minutes of being attached to the net)		VII.f,x			II.c.						
Social Engineering	V.a	VII.b,i	IV	II.l	II.c.						
Events that indicate an attack is/has happened			XIII.m.	I.j,l, VIII.a,i	VII						
Legal Issues	V.h		I.f	I.h,ii	III						
Attack surfaces / vectors		V.c,i	III, XI	I.b.	II.c,d.						
Attack trees				I.c.	IV.l.						
Insider problem			IX	VIII.c.vii,ix	XI.f.						
Covert Channels		VII.b,vi,vii		VI.b.xii							
Threat Information Sources (e.g., CERT)			III.a.		IV.g						
Outcomes											
Students will be able to:											
Students will be able to identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations, aversion to risk	V.a		III	I.b,i	II.c,d.						
Students will be able to describe different types of attacks and their characteristics		II.c	III.j., XII.r.	V	II.c.						

NSA/DHS CAE-IA/CD Knowledge Units - Core 2Y

		Courses	CIS 146	CIS 280	CIS 214	CIS 245	CIS 246					
Click here to return to KU Listing				(Click Here) READ THIS FIRST: This matrix is for th								
Fundamental Security Design Principles												
Provide students with basic security design fundamentals that help create systems that are worthy of being trusted.												
	Topics											
		Separation (of domains)		IV.g,a,b NIST Pubs 800-14 and 800-27								
		Isolation		IV.g,a,b NIST Pubs 800-14 and 800-27								
		Encapsulation		IV.g,a,b NIST Pubs 800-14 and 800-27								
		Least Privilege		IV.g,a,b NIST Pubs 800-14 and 800-27								
		Simplicity (of design)		IV.g,a,b NIST Pubs 800-14 and 800-27								
		Minimization (of implementation)		IV.g,a,b NIST Pubs 800-14 and 800-27								
		Fail Safe Defaults / Fail Secure		IV.g,a,b NIST Pubs 800-14 and 800-27								
		Modularity		IV.g,a,b NIST Pubs 800-14 and 800-27								
		Layering		IV.g,a,b NIST Pubs 800-14 and 800-27								
		Least Astonishment		IV.g,a,b NIST Pubs 800-14 and 800-27			I.g					
		Open Design		IV.g,a,b NIST Pubs 800-14 and 800-27		XII						
		Usability		IV.g,a,b NIST Pubs 800-14 and 800-27		VII	I.h					
	Outcomes											
Students will be able to:												
		List the first principles of security		IV.g,a,b NIST Pubs 800-14 and 800-27								
		Describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies		IV.g,a,b NIST Pubs 800-14 and 800-27								
		Analyze common security failures and identify specific design principles that have been violated		IV.g,a,b NIST Pubs 800-14 and 800-27								
		Identify the needed design principle when given a specific scenario		IV.g,a,b NIST Pubs 800-14 and 800-27								
		Describe why good human machine interfaces are important to system use		IV.g,a,b NIST Pubs 800-14 and 800-27	XII		I.g					
		Understand the interaction between security and system usability and the importance for minimizing the affects of security mechanisms		IV.g,a,b NIST Pubs 800-14 and 800-27	VII		I.h					

NSA/DHS CAE-IA/CD Knowledge Units - Core 2Y

		Courses	CIS 146	CIS 280	CIS 214	CIS 245	CIS 246						
Click here to return to KU Listing				(Click Here) READ THIS FIRST: This matri									
Information Assurance Fundamentals Provide students with basic concepts of information assurance fundamentals.													
	Topics												
		Threats and Adversaries		II.c,d		III	I.b,c,d						
		Vulnerabilities and Risks		V		III	I.b,c,d, VI						
		Basic Risk Assessment		V		XIII.m	I.g,h,i						
		Security Life-Cycle		I.j.k									
		Intrusion Detection and Prevention Systems		VII		XIII	III.h,i						
		Cryptography		VIII	IX	XII							
		Data Security (in transmission, at rest, in processing)		I.g, V.a		XII.g							
		Security Models		I.f, IV,X,XII									
		Access Control Models (MAC, DAC, RBAC)		VI.a,b,c,d									
		Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-		VI.c									
		Security Mechanisms (e.g., Identification/Authentication, Audit)		XII.a									
	Outcomes												
	Students will be able to:												
		List the fundamental concepts of the Information Assurance / Cyber Defense discipline		II.c,d		III							
		Describe how the fundamental concepts of cyber defense can be used to provide system security		V		III							
		Examine the architecture of a typical, complex system and identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed		V	IX	XIII.m	I.b,c,d						

NSA/DHS CAE-IA/CD Knowledge Units - Core 2Y

		Courses	CIS 146	CIS 280	CIS 214	CIS 245	CIS 246						
Click here to return to KU Listing				(Click Here) READ THIS FIRST: T									
Introduction to Cryptography Provide students with a basic ability to understand where and how cryptography is used.													
	Topics												
		Symmetric Cryptography (DES, Twofish)		VIII.c		XII.d							
		*Public Key Cryptography											
		Public Key Infrastructure		VIII.f		XII.j							
		Certificates		VIII.h		XII.f							
		*Hash Functions (MD4, MD5, SHA-1, SHA-2, SHA-3)											
		For integrity		VIII.b		XII.h							
		For protecting authentication data		VIII.b		XII.h							
		Collision resistance				XII.g							
		Digital Signatures (Authentication)		VIII.h		XII.f							
		Key Management (creation, exchange/distribution)		VIII.d		XII.i							
		Cryptographic Modes (and their strengths and weaknesses)		VIII.b		XII.n							
		Types of Attacks (brute force, chosen plaintext, known plaintext, differential and		VIII.l		XII.o							
		Common Cryptographic Protocols		VIII.a		XII.a							
		DES -> AES (evolution from DES to AES)		VIII.c		XI.d							
		Security Functions (data protection, data integrity, authentication)		VIII.k		XII.j							
	Outcomes												
	Students will be able to:			VIII.c		XII.d							
		Identify the elements of a cryptographic system											
		Describe the differences between symmetric and asymmetric algorithms		VIII.f		XII.j							
		Describe which cryptographic protocols, tools and techniques are appropriate for a given situation		VIII.h		XII.f							
		Describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation (e.g., key management), etc		VIII.b		XII.h							

NSA/DHS CAE-IA/CD Knowledge Units - Core 2Y

		Courses	CIS 146	CIS 280	CIS 214	CIS 245	CIS 246						
Click here to return to KU Listing				(Click Here) READ THIS FIRST: This									
Information Technology System Components													
Provide students with an understanding of the basic components in an information technology system and their roles in system operation.													
	Topics												
		Workstations	I			VIII							
		Servers	I			VIII							
		Network Storage Devices	II			VIII.b,t							
		Routers / Switches / Gateways	IV			XIII							
		Guards / CDSes / VPNs / Firewalls	IV	VII		XIII.e							
		IDSes, IPSes		VII	IV.i	XIII.j	III.i						
		Mobile Devices				IX	I.i.vi,V.e						
		Peripheral Devices / Security Peripherals	IV	VII,IX		XIII							
	Outcomes												
	Students will be able to:		I										
		Students will be able to describe the hardware components of modern computing environments and their individual functions.	I	VII	IV.i	VIII	III.i						

NSA/DHS CAE-IA/CD Knowledge Units - Core 2Y

			Courses	CIS 146	CIS 280	CIS 214	CIS 245	CIS 246						
Click here to return to KU Listing					(Click Here) READ THIS FIRST: Th									
Networking Concepts														
Provide students with basic understanding of network components and how they interact.														
	Topics													
		Overview of Networking (OSI Model)					II.a-g							
		Network Media		IV. d										
		Network architectures (LANs, WANs)		IV.a										
		Network Devices (Routers, Switches, VPNs, Firewalls)		IV.f	VI, VII	VII	XIII.a-o							
		Network Services					VI.b-g							
		Network Protocols (TCP/IP, HTTP, DNS, SMTP, UDP)		IV.e			IV. e-g							
		Network Topologies		IV.b										
		Overview of Network Security Issues		V	II.c,d		III							
	Outcomes													
	Students will be able to:													
		Describe the fundamental concepts, technologies, components and issues related to communications and data networks		IV. d	VI, VII	VII	II.a-g							
		Describe a basic network architecture given a specific need and set of hosts/clients		IV.a										
		Track and identify the packets involved in a simple TCP connection (or a trace of such a connection)		IV.f										
		Use a network monitoring tool (e.g., WireShark)					XIII.a-o							
		Use a network mapping tool (e.g., Nmap).		IV.e	II.c,d		VI.b-g							

NSA/DHS CAE-IA/CD Knowledge Units - Core 2Y

Courses	CIS 146	CIS 280	CIS 214	CIS 245	CIS 246						
Click here to return to KU Listing		(Click Here) READ THIS FIRST: T									
Policy. Legal, Ethics and Compliance Provide students with and understanding of information assurance in context and the rules and guidelines that control them.											
Topics											
HIPAA / FERPA	III.h	III.e			I.I.iii						
Computer Security Act		III.d									
Sarbanes – Oxley	III.h	III.h			I.I.iv						
Gramm – Leach – Bliley		III.h									
Privacy (COPPA)		III.e									
Payment Card Industry Data Security Standard (PCI DSS)					I.I.i						
State, US and international standards / jurisdictions		III.j			I.I.vi						
Laws and Authorities	III.h	III.a,j									
US Patriot Act	III.h	III.d									
Bring Your Own Device (BYOD) issues					VI.i						
Americans with Disabilities Act, Section 508		III.d.a									
Outcomes											
Students will be able to:											
List the applicable laws and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data	III.h	III.e			I.I.iii						
Describe their responsibilities related to the handling of information about vulnerabilities		III.d									
Describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it	III.h	III.h			I.I.iv						

NSA/DHS CAE-IA/CD Knowledge Units - Core 2Y

Courses	CIS 146	CIS 280	CIS 214	CIS 245	CIS 246						
Click here to return to KU Listing		(Click Here) READ THIS FIRST: This									
Systems Administration Provide students with skill to perform basic operations involved in system administration.											
Topics											
OS Installation				VIII.a.i							
User accounts management		VIII.a.i		VIII.g	V.e.iv,v						
Password policies		VIII.g		VIII.k,n	V.e.iv,v						
Authentications Methods		VIII.k,n		VIII.k	V.d						
Command Line Interfaces	III.b	VIII.k		VIII.b-g							
Configuration Management		VIII.b-g		VIII.n							
Updates and patches		VIII.n		VIII.o							
Access Controls		VIII.o		VIII.s							
Logging and Auditing (for performance and security)		VIII.s		VIII.q							
Managing System Services		VIII.q		VIII.r							
Virtualization	I.b	VIII.r		VIII.s.i							
Backup and Restoring Data	III.c	VIII.s.i									
File System Security				VIII.b							
Network Configuration (port security)		VIII.b		VIII.r							
Host (Workstation/Server) Intrusion Detection		VIII.r		XIII.k							
Security Policy Development		XIII.k			I,h						
Outcomes											
Students will be able to:											
Apply the knowledge gained to successfully install and securely configure, operate and maintain a commodity OS, to include: setting up user accounts, configuring appropriate authentication policies, configuring audit capabilities, performing back-ups, installing patches and updates, reviewing security logs, and restoring the system from a backup	III.b	VIII.a.i		VIII.a.i	V.e.iv,v						