Annual Careers in Cybersecurity Workshop for Guidance Counselors

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

▷*National Cybersecurity Workforce Framework*◁

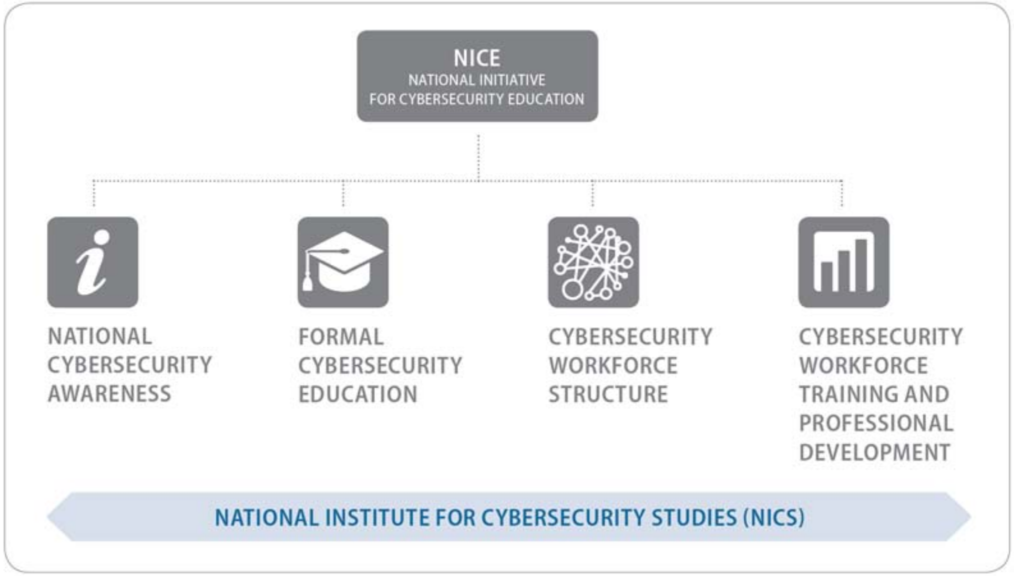
9/27/11

Peggy Maxson, DHS, Director of National Cybersecurity Education Strategy

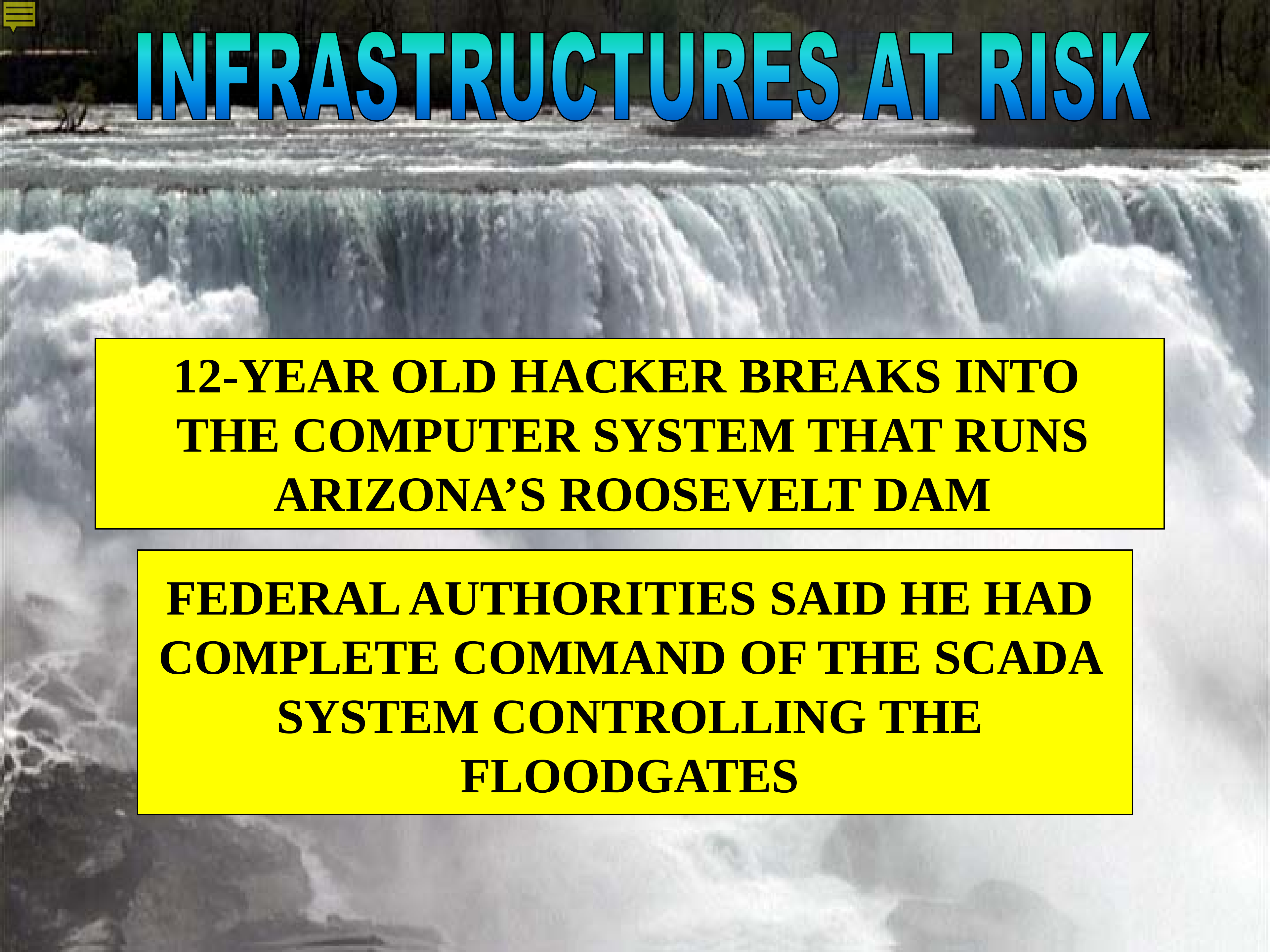
A National Problem

- The Nation needs greater cybersecurity awareness
- The US work force lacks cyber security experts
- Many cybersecurity training programs exist but lack consistency among programs
- Potential employees lack information about skills and abilities for cybersecurity jobs
- Resources exist for teachers and students about cybersecurity but are difficult to find
- Cybersecurity Career development and scholarships are available but uncoordinated
- Lack of communication between government, private industry, and academia

NICE was established to create a cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security.


NICE
NATIONAL INITIATIVE
FOR CYBERSECURITY EDUCATION
NATIONAL CYBERSECURITY AWARENESS
FORMAL CYBERSECURITY EDUCATION
CYBERSECURITY WORKFORCE STRUCTURE
CYBERSECURITY WORKFORCE TRAINING AND PROFESSIONAL DEVELOPMENT
NATIONAL INSTITUTE FOR CYBERSECURITY STUDIES (NICS)

INFRASTRUCTURES AT RISK



12-YEAR OLD HACKER BREAKS INTO THE COMPUTER SYSTEM THAT RUNS ARIZONA’S ROOSEVELT DAM

FEDERAL AUTHORITIES SAID HE HAD COMPLETE COMMAND OF THE SCADA SYSTEM CONTROLLING THE FLOODGATES

INTERVIEW WITH CONVICTED HACKER ROBERT MOORE

Moore tells how he easily broke into 15 telecommunications companies and hundreds of businesses worldwide

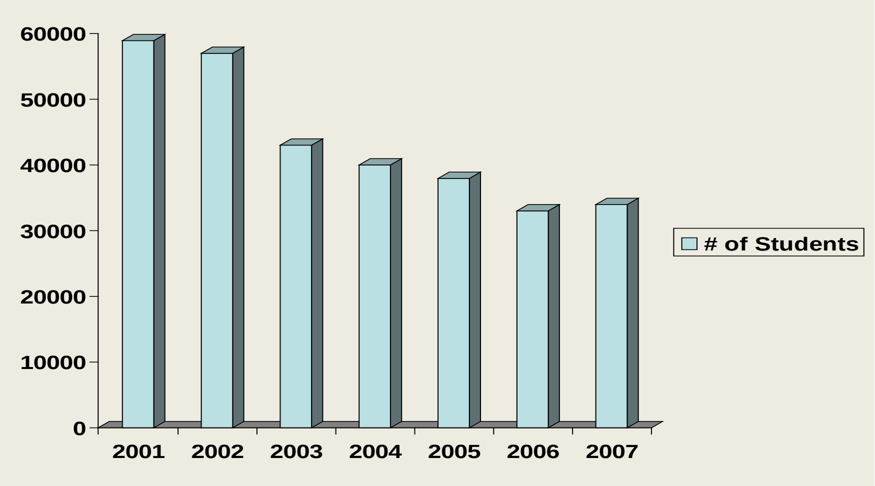
laughing…"It's so easy a caveman can do it."

ESTONIA HIT BY RUSSIAN BASED CYBER ATTACK

- Attacks began April 27, 2007 protesting the relocation of a Soviet-era Bronze Soldier statue
- Peaked during the 8 - 9 May celebration of Soviet victory in WW-II
- Tied up Estonian cyber infrastructure:
  - Telephone exchanges, government ministries, banks, newspapers, fire and ambulance services and broadcasting centers

The Challenge

Computing and Information Sciences
as Intended Major on SAT



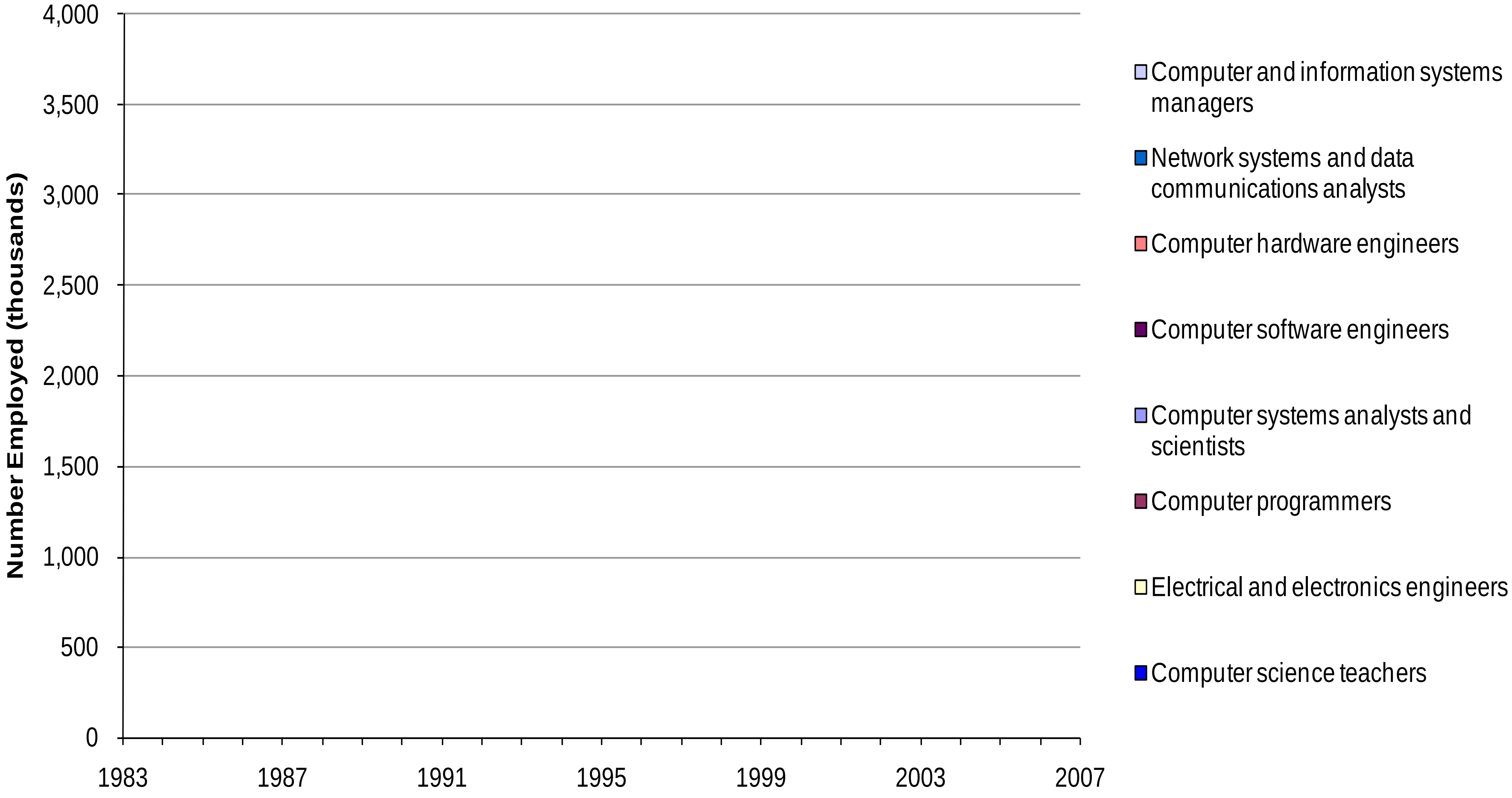
(IT Business Advocacy Roundtable (2008))

TIMSS Mathematics Test Score Comparison (2007):
Avg. = 500 Source: *TIMSS* (2007)

Grade	Four		Grade	Eight
Country	Score		Country	Score
Hong Kong	607		Chinese Taipei	598
Singapore	599		Rep. of Korea	597
Chinese Taipei	576		Singapore	593
Japan	568		Hong Kong	572
Kazakhstan	549		Japan	570
Russian Federat.	544		Hungary	517
England	541		England	513
Latvia	537		Russian Federat.	512
Netherlands	535		United States	508
Lithuania	530		Lithuania	506
United States	529		Czech Republic	504

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

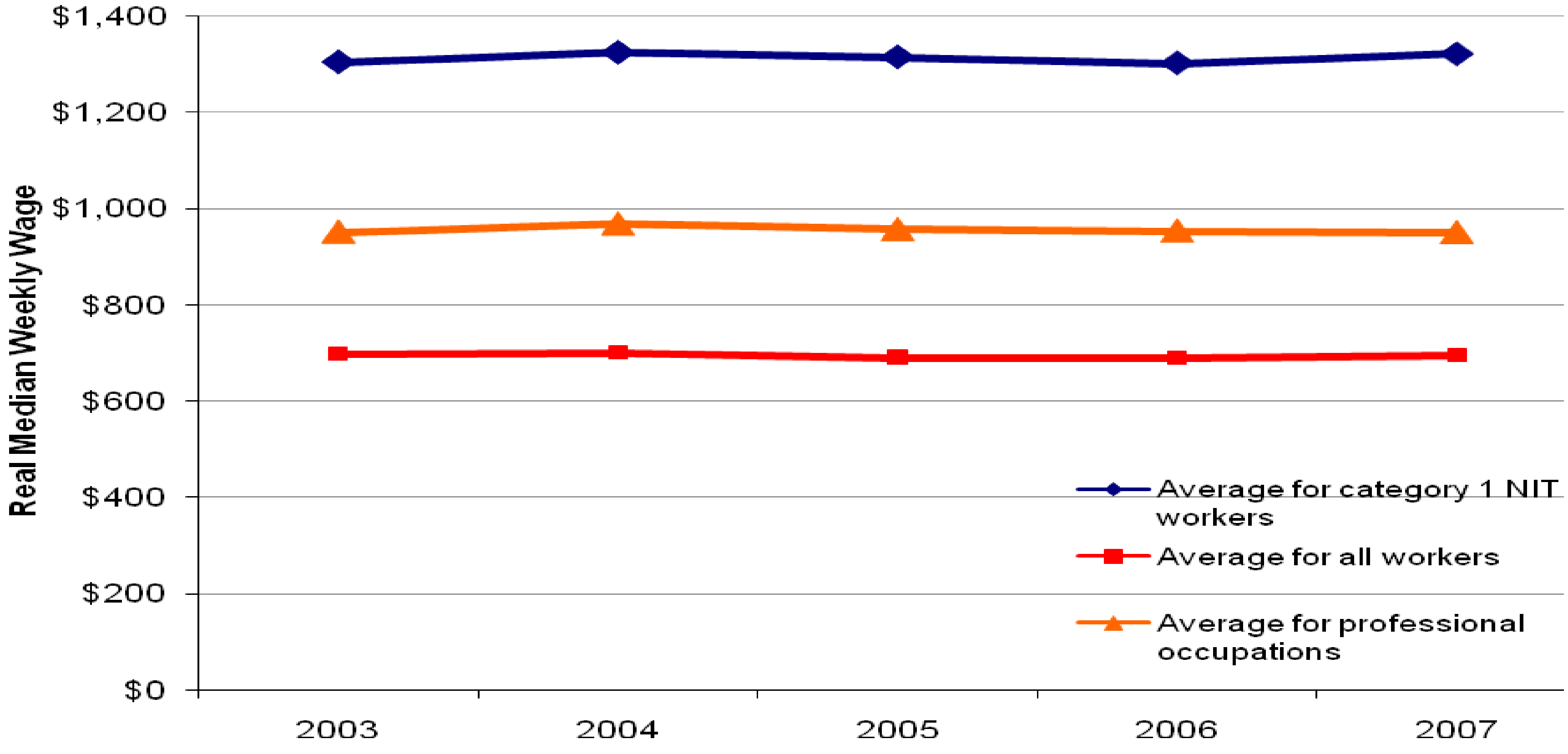
Category 1 NIT Labor Force in Thousands (1983-2007)



Source: Current Population Survey

Network and Information Technology Occupations Real Earnings

NIT Occupations Real Earnings Trends (2003-2007)



Source: Current Population Survey and Consumer Price Index (2007 dollars)

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

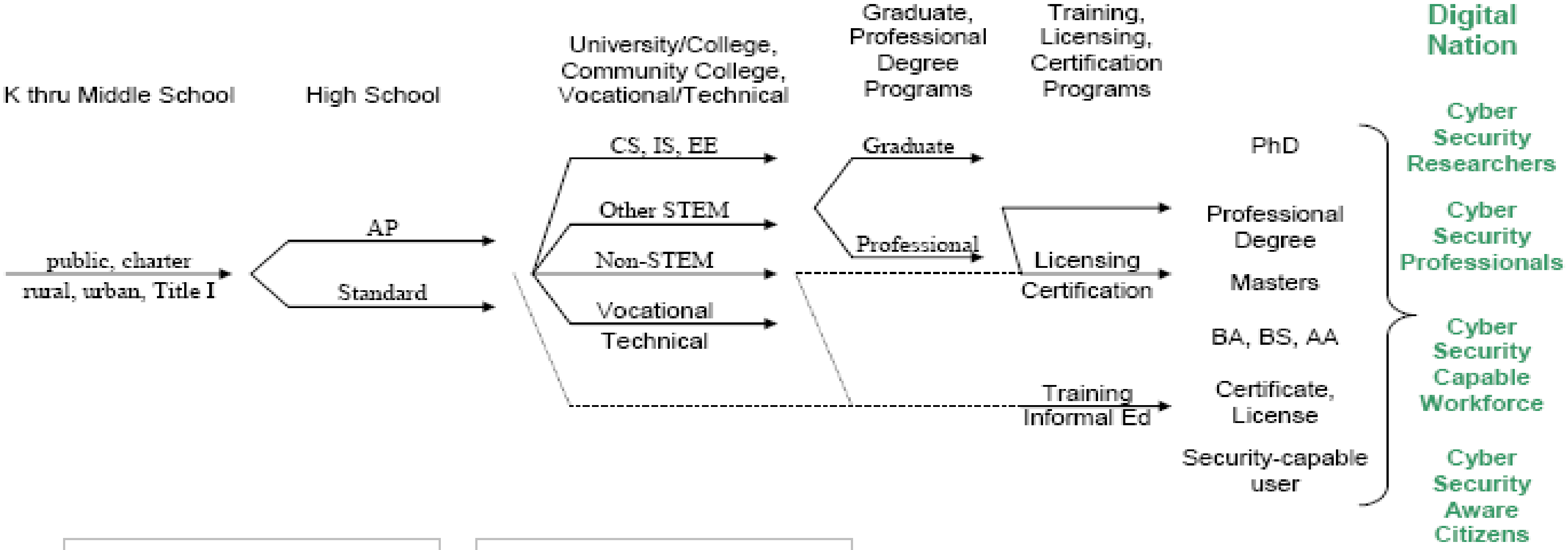
NIT Occupational Growth Projections

Occupational Category	BLS 2006 (thousands)	BLS 2016 (thousands)	% Growth	Total Job Openings (thousands)
Computer systems analysts and scientists	665	838	23%	349
Computer and information scientists, research	25	31	21%	12
Computer systems analysts	504	650	29%	280
Computer specialists	136	157	15%	57
Computer programmers	435	417	-4%	91
Electrical and electronics engineers	291	306	6%	82
Computer software engineers	857	1,181	38%	449
Computer hardware engineers	79	82	5%	28
Network systems and data communications analysts	262	402	**53%**	193
Computer and information systems managers	264	307	16%	86
Category 1 NIT Occupations	**2,853**	**3,533**	**24%**	**1,278**
Professional Occupations	**29,819**	**34,790**	**17%**	**11,067**
All Occupations	**150,620**	**166,220**	**10%**	**50,732**

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Source: Bureau of Labor Statistics

The Pipeline



K thru Middle School

High School

University/College, Community College, Vocational/Technical

Graduate, Professional Degree Programs

Training, Licensing, Certification Programs

Digital Nation

public, charter

rural, urban, Title I

AP

Standard

CS, IS, EE

Other STEM

Non-STEM

Vocational Technical

Graduate

Professional

Licensing Certification

Training Informal Ed

PhD

Professional Degree

Masters

BA, BS, AA

Certificate, License

Security-capable user

Cyber Security Researchers

Cyber Security Professionals

Cyber Security Capable Workforce

Cyber Security Aware Citizens

Pipeline Stakeholders:

- Students
- Parents
- Teachers
- Educational Institutions
- State, Local Government
- Professional Organizations
- Commercial Sector
- Federal Government

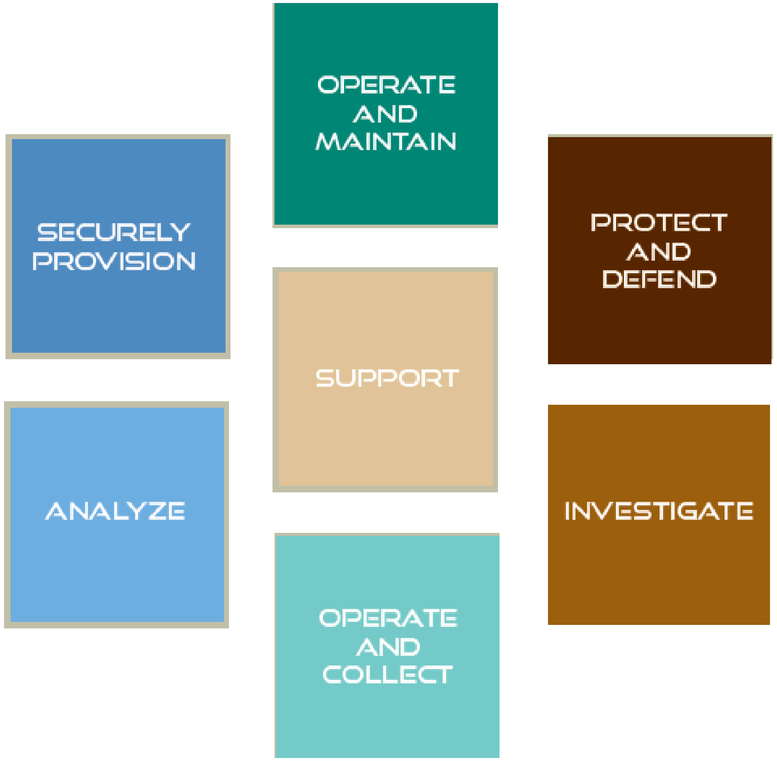
Pipeline Substrates:

- Curriculum
- Ontologies, Taxonomies
- Standards
- Teacher Preparation
- Public Awareness
- Education Technologies
- Science and Practice of Learning

Framework Categories

The **Framework** *organizes cybersecurity into* ***seven*** *high-level categories, each comprised of several specialty areas.*

Interactive PDF at:
http://csrc.nist.gov/nice/framework/



OPERATE AND MAINTAIN

SECURELY PROVISION

PROTECT AND DEFEND

SUPPORT

ANALYZE

INVESTIGATE

OPERATE AND COLLECT

CYBERSECURITY WORKFORCE FRAMEWORK

7 Categories - Defined

Securely Provision	Specialty areas concerned with conceptualizing, designing, and building secure IT systems.
Operate and Maintain	Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.
Protect and Defend	Specialty area responsible for the identification, analysis and mitigation of threats to IT systems and networks.
Investigate	Specialty areas responsible for the investigation of cyber events or crimes which occur within IT Systems and networks.
Operate and Collect	Specialty areas responsible for the highly specialized and largely classified collection of cybersecurity information that may be used to develop intelligence.
Analyze	Specialty area responsible for highly specialized and largely classified review and evaluation of incoming cybersecurity information.
Support	Specialty areas that provide critical support so that others may effectively conduct their cybersecurity work.

Category: Operate and Maintain

Specialty Area: Systems Security Analysis

Responsible for the integration/testing, operations and maintenance of systems security

Typical OPM Classification: 2210, Information Technology Management *(Actual information provided by OPM)*

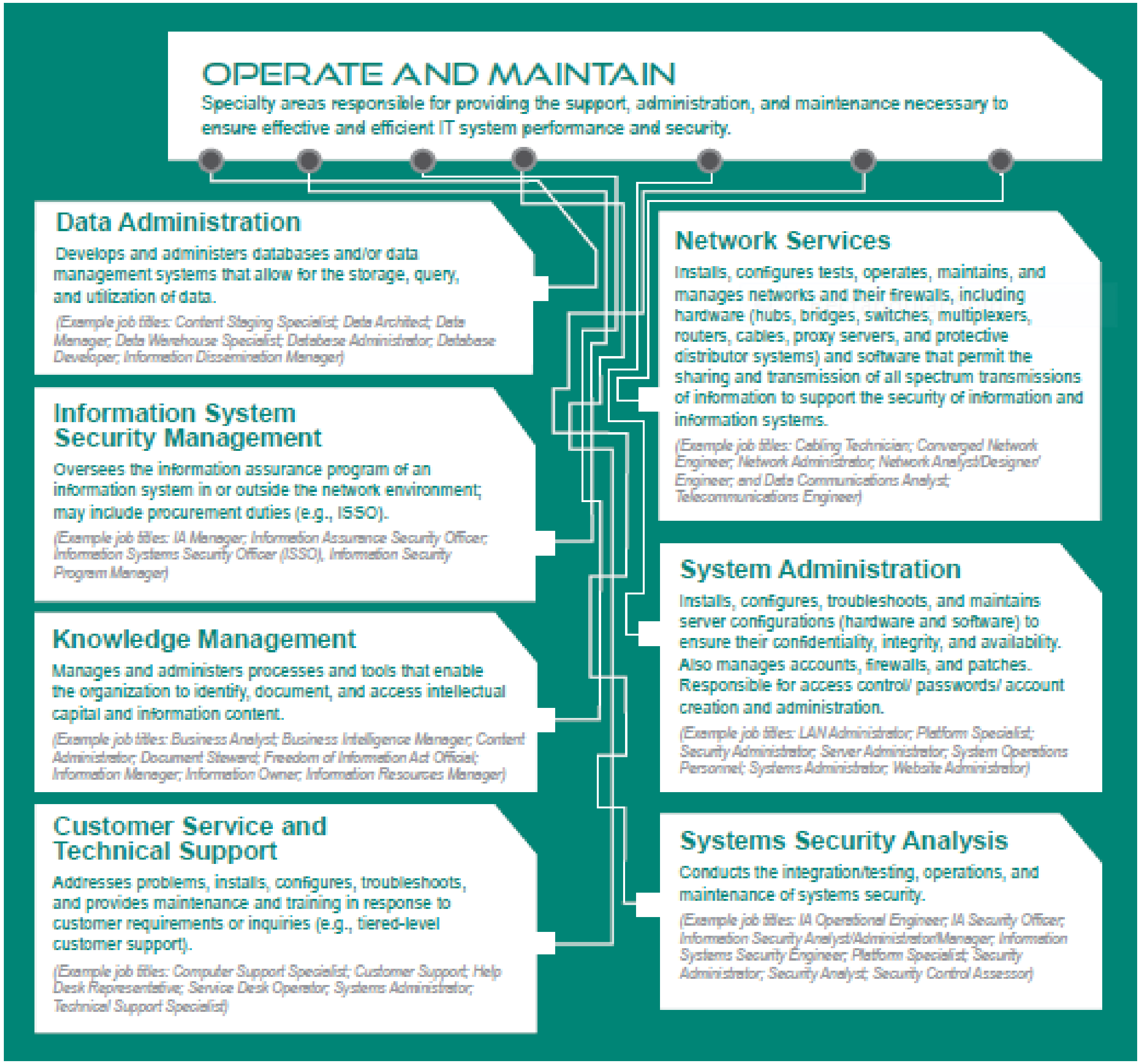
Example Job Titles: Information Assurance Security Information Systems Security
Information System Security IA Operational Engineer

Job Tasks

1. Implement system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.
2. Implement approaches to resolve vulnerabilities, mitigate risks and recommend security changes to system or system components as needed.
3. Perform security reviews and identify security gaps in security architecture resulting in recommendations for the inclusion into the risk mitigation strategy.
4. Etc…..

Competency	KSA
Information Assurance: Knowledge of methods and procedures to protect information systems and data by ensuring their availability, authentication, confidentiality and integrity.	Skill in determining how a security system should work.
	Knowledge of security management
	Knowledge of Information Assurance principles and tenets.
Risk Management: Knowledge of the principles, methods, and tools used for risk assessment and mitigation, including assessment of failures and their consequences.	Knowledge of risk management processes, including steps and methods for assessing risk.
	Knowledge of network access and authorization (e.g. PKI)
	Skill in, assessing the robustness of security systems and designs.
System Life Cycle: Knowledge of systems life cycle management concepts used to plan, develop, implement, operate and maintain information systems.	Knowledge of system lifecycle management principals.
	Knowledge of how system components are installed, integrated and optimized.
	Skill in designing the integration of hardware and software solutions.

Specialty Areas (SAs)



OPERATE AND MAINTAIN

Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.

Data Administration

Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

(Example job titles: Content Staging Specialist; Data Architect; Data Manager; Data Warehouse Specialist; Database Administrator; Database Developer; Information Dissemination Manager)

Information System Security Management

Oversees the information assurance program of an information system in or outside the network environment; may include procurement duties (e.g., ISSO).

(Example job titles: IA Manager; Information Assurance Security Officer; Information Systems Security Officer (ISSO), Information Security Program Manager)

Knowledge Management

Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

(Example job titles: Business Analyst; Business Intelligence Manager; Content Administrator; Document Steward; Freedom of Information Act Official; Information Manager; Information Owner; Information Resources Manager)

Customer Service and Technical Support

Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

(Example job titles: Computer Support Specialist; Customer Support; Help Desk Representative; Service Desk Operator; Systems Administrator; Technical Support Specialist)

Network Services

Installs, configures tests, operates, maintains, and manages networks and their firewalls, including hardware (hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

(Example job titles: Cabling Technician; Converged Network Engineer; Network Administrator; Network Analyst/Designer/ Engineer; and Data Communications Analyst; Telecommunications Engineer)

System Administration

Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control/ passwords/ account creation and administration.

(Example job titles: LAN Administrator; Platform Specialist; Security Administrator; Server Administrator; System Operations Personnel; Systems Administrator; Website Administrator)

Systems Security Analysis

Conducts the integration/testing, operations, and maintenance of systems security.

(Example job titles: IA Operational Engineer; IA Security Officer; Information Security Analyst/Administrator/Manager; Information Systems Security Engineer; Platform Specialist; Security Administrator; Security Analyst; Security Control Assessor)

NICE
NATIONAL INITIATIVE FOR **CYBER**SECURITY EDUCATION

NICE Cybersecurity Specialties Framework

The 31 Cybersecurity Specialties:

Securely Provision

- Systems Requirements Planning
- Systems Development
- Software Engineering
- Enterprise Architecture
- Test and Evaluation
- Technology Demonstration
- Information Assurance Compliance

Operate and Maintain

- System Administration
- Network Services
- Systems Security Analysis
- Customer Service and Technical Support
- Data Administration
- Knowledge Management
- Information Systems Security Management

Support

- Legal Advice and Advocacy
- Education and Training
- Strategic Planning and Policy Development

Protect and Defend

- Computer Network Defense Infrastructure Support
- Vulnerability Assessment and Management
- Incident Response
- Computer Network Defense
- Security Program Management

Investigate

- Investigation
- Digital Forensics

Operate and Collect

- Collection Operations
- Cyber Operations Planning
- Cyber Operations

Analyze

- Cyber Threat Analysis
- Exploitation Analysis
- Targets
- All Source Intelligence

Framework example

The 31 Cybersecurity Specialties:

Securely Provision

- Systems Requirements Planning
- Systems Development
- Software Engineering
- Enterprise Architecture
- Test and Evaluation
- Technology Demonstration
- Information Assurance Compliance

Operate and Maintain

- System Administration
- Network Services
- Systems Security Analysis
- Customer Service and Technical Support
- Data Administration
- Knowledge Management
- Information Systems Security Management

Support

- Legal Advice and Advocacy
- Education and Training
- Strategic Planning and Policy Development

Protect and Defend

- Computer Network Defense Infrastructure Support
- Vulnerability Assessment and Management
- Incident Response
- Computer Network Defense
- Security Program Management

Investigate

- Investigation
- Digital Forensics

Operate and Collect

- Collection Operations
- Cyber Operations Planning
- Cyber Operations

Analyze

- Cyber Threat Analysis
- Exploitation Analysis
- Targets
- All Source Intelligence

Framework Definition Example

Specialty	Sample Job Titles
Data Administration - develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.	-Data warehouse specialist -Database developer -Database administrator -Data architect -Information dissemination manager -Content staging specialist -Data manager -Systems operations personnel

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Framework Tasks Example

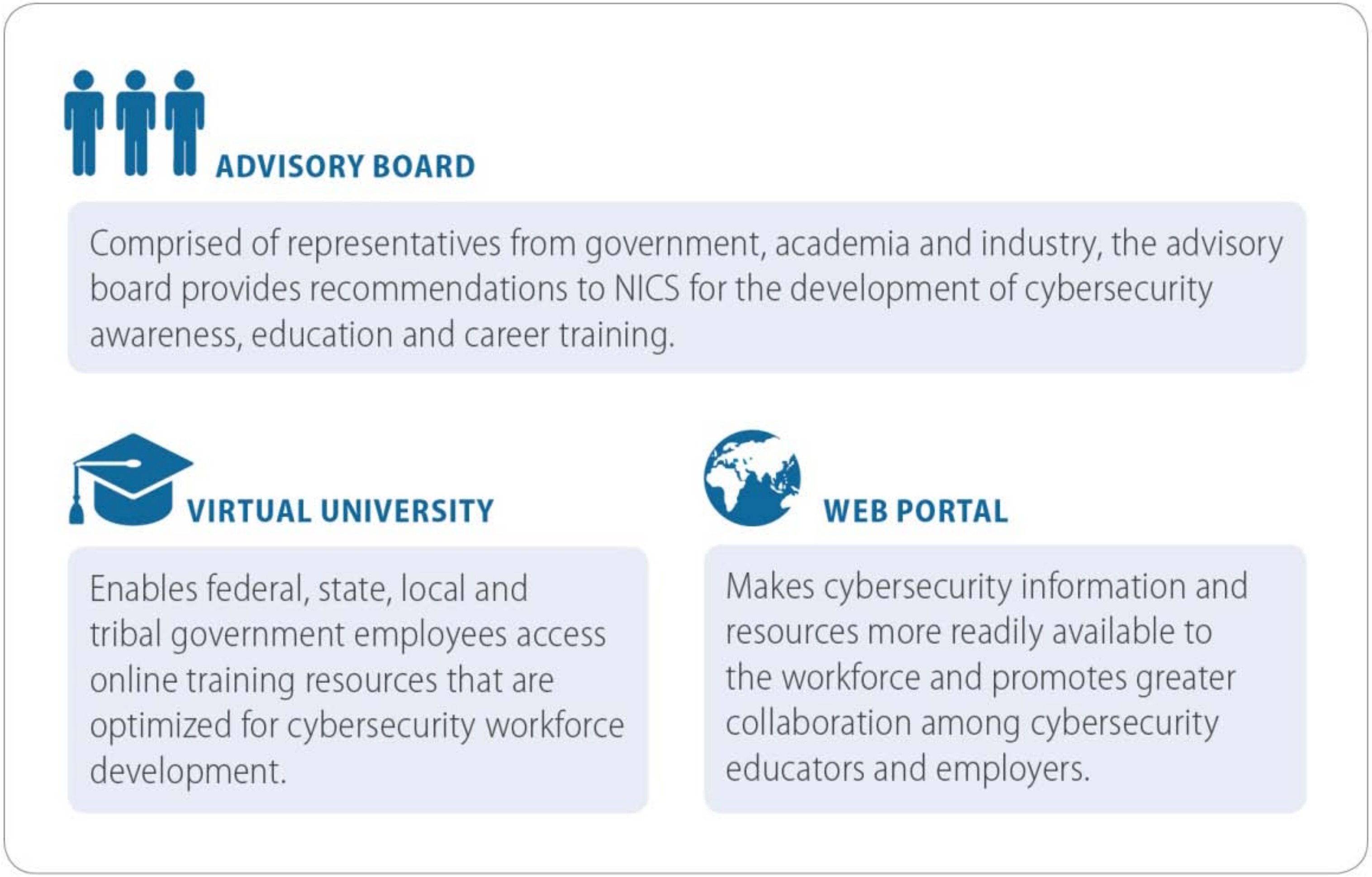
Data Administration	Task	Analyze and define data requirements and specifications
Data Administration	Task	Analyze and plan for anticipated changes in data capacity requirements
Data Administration	Task	Design and implement database systems
Data Administration	Task	Develop and implement data mining and data warehousing programs
Data Administration	Task	Develop data standards, policies, and procedures
Data Administration	Task	Install and configure database management systems software
Data Administration	Task	Maintain assured message delivery systems
Data Administration	Task	Maintain database management systems software
Data Administration	Task	Maintain directory replication services that enables information to replicate automatically from rear servers to forward units via optimized routing
Data Administration	Task	Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required
Data Administration	Task	Manage the compilation, cataloging, caching, distribution, and retrieval of data
Data Administration	Task	Monitor and maintain databases to ensure optimal performance
Data Administration	Task	Perform backup and recovery of databases to ensure data integrity
Data Administration	Task	Provide a managed flow of relevant information (via web-based portals or other means) based on a mission requirements
Data Administration	Task	Provide recommendations on new database technologies and architectures

Framework KSAs Example

Linked to OPM Competency:

Data Administration	KSA	Knowledge of data administration and data standardization policies and standards	Data Management
Data Administration	KSA	Knowledge of data backup and recovery concepts and tool, including different types of backups (e.g., full, incremental)	Computer Forensics
Data Administration	KSA	Knowledge of data mining and data warehousing principles	Data Management
Data Administration	KSA	Knowledge of database management systems, query languages, table relationships, and views	Database Management Systems
Data Administration	KSA	Knowledge of digital rights management	Encryption
Data Administration	KSA	Knowledge of agency LAN/WAN pathways	Infrastructure Design
Data Administration	KSA	Knowledge of enterprise messaging systems and associated software	Enterprise Architecture
Data Administration	KSA	Knowledge of network access and authorization (e.g., public key infrastructure)	Identity Management
Data Administration	KSA	Knowledge of operating systems	Operating Systems
Data Administration	KSA	Knowledge of policy-based and risk adaptive access controls	Identity Management
Data Administration	KSA	Knowledge of query languages such as SQL (structured query language)	Database Management Systems
Data Administration	KSA	Knowledge of sources, characteristics, and uses of the organization's data assets	Data Management
Data Administration	KSA	Knowledge of telecommunications concepts	Telecommunications
Data Administration	KSA	Knowledge of the characteristics of physical and virtual data storage media	Data Management
Data Administration	KSA	Skill in allocating storage capacity in the design of data management systems	Database Administration
Data Administration	KSA	Skill in designing databases	Database Administration
Data Administration	KSA	Skill in developing data dictionaries	Data Management
Data Administration	KSA	Skill in developing data models	Modeling and Simulation
Data Administration	KSA	Skill in developing data repositories	Data Management
Data Administration	KSA	Skill in generating queries and reports	Database Management Systems
Data Administration	KSA	Skill in maintaining databases	Database Management Systems
Data Administration	KSA	Skill in optimizing database performance	Database Administration
Data Administration	KSA	Knowledge of database theory	Data Management

THREE ELEMENTS OF THE NICS APPROACH



ADVISORY BOARD

Comprised of representatives from government, academia and industry, the advisory board provides recommendations to NICS for the development of cybersecurity awareness, education and career training.

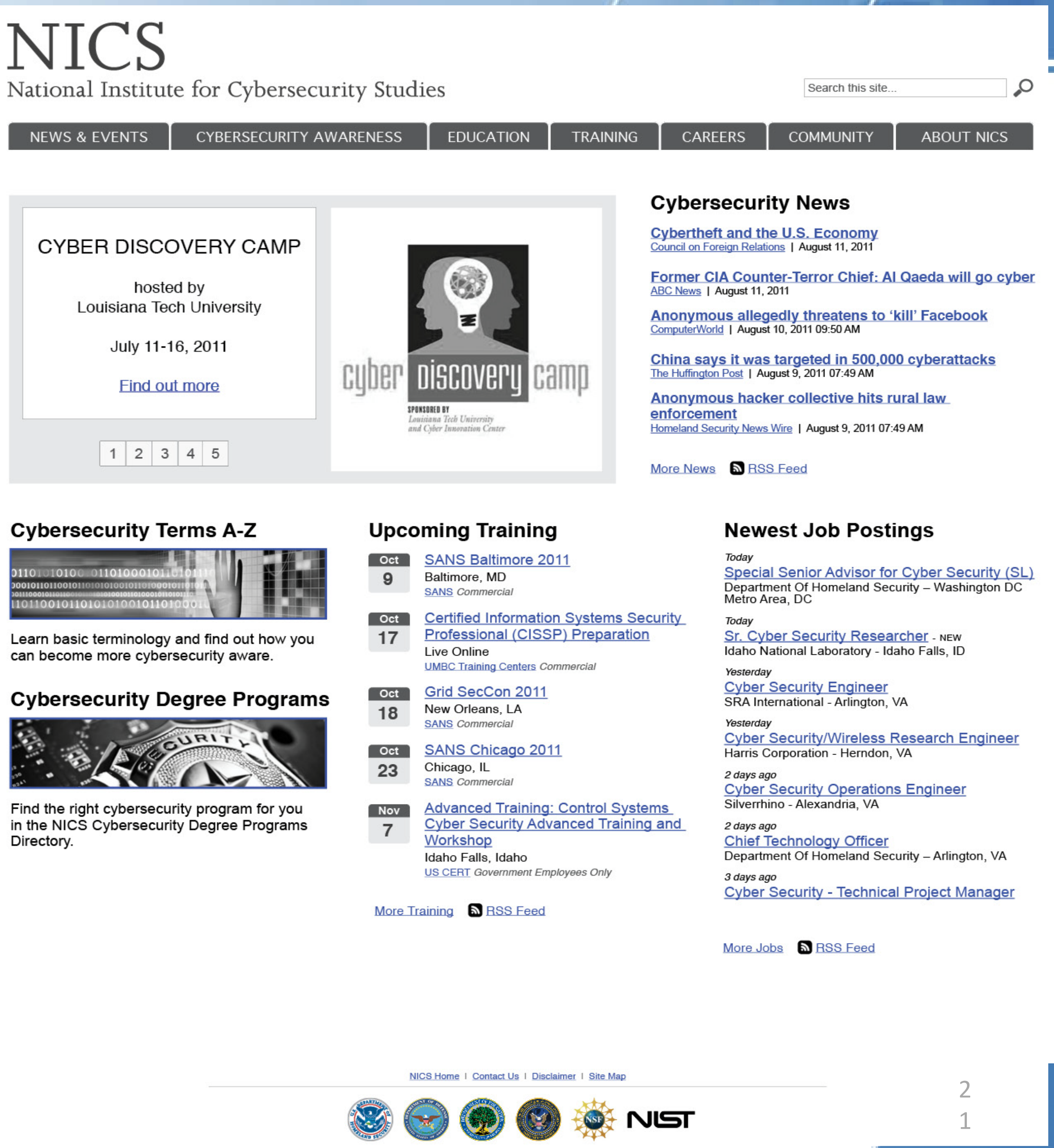
VIRTUAL UNIVERSITY

Enables federal, state, local and tribal government employees access online training resources that are optimized for cybersecurity workforce development.

WEB PORTAL

Makes cybersecurity information and resources more readily available to the workforce and promotes greater collaboration among cybersecurity educators and employers.

Draft NICS Portal Homepage



NICS

National Institute for Cybersecurity Studies

CYBER DISCOVERY CAMP

hosted by
Louisiana Tech University

July 11-16, 2011

Find out more

Cybersecurity News

Cybertheft and the U.S. Economy
Council on Foreign Relations | August 11, 2011

Former CIA Counter-Terror Chief: Al Qaeda will go cyber
ABC News | August 11, 2011

Anonymous allegedly threatens to 'kill' Facebook
ComputerWorld | August 10, 2011 09:50 AM

China says it was targeted in 500,000 cyberattacks
The Huffington Post | August 9, 2011 07:49 AM

Anonymous hacker collective hits rural law enforcement
Homeland Security News Wire | August 9, 2011 07:49 AM

More News RSS Feed

Cybersecurity Terms A-Z

Learn basic terminology and find out how you can become more cybersecurity aware.

Cybersecurity Degree Programs

Find the right cybersecurity program for you in the NICS Cybersecurity Degree Programs Directory.

Upcoming Training

Oct 9 — SANS Baltimore 2011
Baltimore, MD
SANS *Commercial*

Oct 17 — Certified Information Systems Security Professional (CISSP) Preparation
Live Online
UMBC Training Centers *Commercial*

Oct 18 — Grid SecCon 2011
New Orleans, LA
SANS *Commercial*

Oct 23 — SANS Chicago 2011
Chicago, IL
SANS *Commercial*

Nov 7 — Advanced Training: Control Systems Cyber Security Advanced Training and Workshop
Idaho Falls, Idaho
US CERT *Government Employees Only*

More Training RSS Feed

Newest Job Postings

Today
Special Senior Advisor for Cyber Security (SL)
Department Of Homeland Security – Washington DC Metro Area, DC

Today
Sr. Cyber Security Researcher - NEW
Idaho National Laboratory - Idaho Falls, ID

Yesterday
Cyber Security Engineer
SRA International - Arlington, VA

Yesterday
Cyber Security/Wireless Research Engineer
Harris Corporation - Herndon, VA

2 days ago
Cyber Security Operations Engineer
Silverrhino - Alexandria, VA

2 days ago
Chief Technology Officer
Department Of Homeland Security – Arlington, VA

3 days ago
Cyber Security - Technical Project Manager

More Jobs RSS Feed

NICS Home | Contact Us | Disclaimer | Site Map

Comments to:
NICS@dhs.gov

Centers of Academic Excellence

- 145 Schools Nationwide http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml
- Within Maryland:
  - Anne Arundel Community College (2Y)
  - Bowie State University
  - Capitol College
  - College of Southern Md (2Y)
  - Johns Hopkins University
  - Hagerstown Community College (2Y)
  - Prince Georges Community College (2Y)
  - The Community College of Baltimore County (2Y)
  - Towson University
  - United States Naval Academy
  - University of Maryland, Baltimore County
  - University of Maryland, College Park
  - University of Maryland University College

Information Security Crime Investigator/Forensics Expert

“The thrill of the hunt! You never encounter the same crime twice!”

You are a criminal investigator who analyzes how intruders breached the infrastructure, and you get to see the bad guys go to jail.

www.sans.org

System, Network and/or Web Penetration Tester

Find security vulnerabilities in infrastructure and support stronger security solutions.

You can use hacker skills, legally!

www.sans.org

Forensic Analyst

“It’s CSI for cyber geeks! It’s like being one of the good spies on James Bond. The ultimate techno-dude!”

This job requires the analyst to “go deep” into a system, find out what went wrong, what’s still wrong, and trace it.

www.sans.org

Cybersecurity Workforce Structure, Training and Professional Development

… Discussion ...

Peggy Maxson – margaret.maxson@dhs.gov

QUESTIONS?