

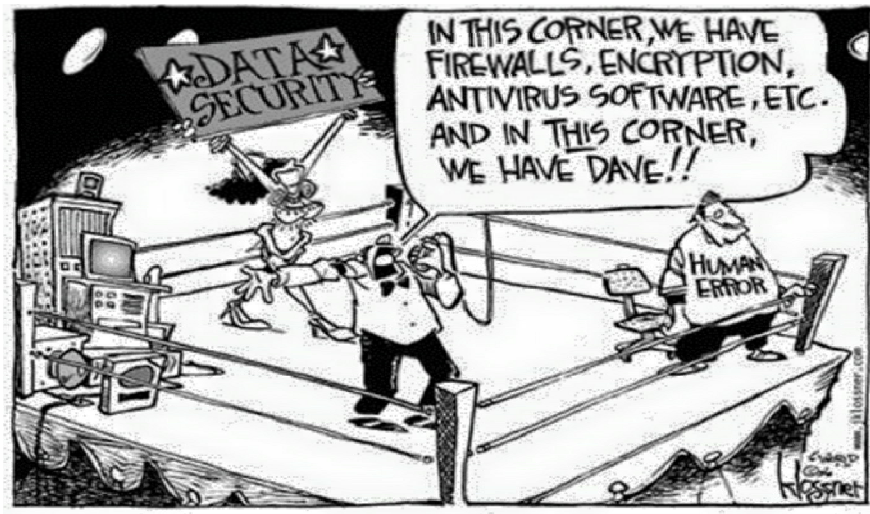


### ARE YOU THE NEXT CYBER WARRIOR?

*Maria S. Thompson  
State Chief Risk/Security Officer*



### Which Side Are You On?



## Cyber Professionals Deficiency Statistics

- Cybersecurity job postings grew 74% from 2007 to 2013. Twice the growth of any IT jobs.
- U.S. employers posted 50,000 jobs requesting CISSP credentials in 2013, a year in which the population of CISSP holders numbered 60,000
- Research findings from Frost & Sullivan stated the labor gap in IT security could grow to as much as 1.5 million in five years. "The demand for the (cybersecurity) workforce is expected to rise to 6 million (globally) by 2019."
- "It's probably 10- to 12-times harder to find cybersecurity professionals than it is to find general IT professionals,"
- Trendmicro estimates that growth of cybersecurity positions is currently increasing at a rate 12 times faster than the rest of the U.S. job market



## What Employers Are Looking For

### Knowledge, Skills and Abilities:

- On the strategic side, "you need people who can do more than configure rules and policies and 'keep the bad guys out.' You need data scientists. You need people with different backgrounds. You need people who can look at large quantities of data and can analyze trends and are good at spotting anomalous behaviors in those data patterns,"
- Experts agree more education and training is critical to increase the candidate ranks. "One of industry biggest concerns, or criticisms, relative to security talent that's coming out of colleges and universities is that ... **the academic learning is terrific, but you really need hands-on experience in cyber security environment,**"
- To do cybersecurity well you need two kinds of qualities that we don't know how to train for," Borg said. "We don't know how to train them to move across many disciplines, many different technical areas. We also don't know how to train people to think like hackers or think outside the box."



## What Employers Are Looking For

### Training & Certification:

Certifications drive starting salaries even higher. In the security category, having a Certified Information Systems Security Professional (CISSP) certification adds 6%, on average, to IT salaries, while Check Point Firewall administration skills are worth a 7% bump, Cisco network administration skills add 9%, and Linux/Unix administration skills add 9% to starting pay.

Certifications are not the end all. A recruiter can find someone to fill a role based on the required certification, however, that certification does not automatically translate to deep security understanding

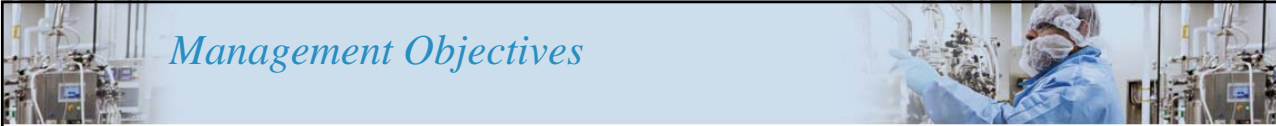


## What Employers Are Saying

### Knowledge, Skills and Abilities:


- There's no silver bullet. Training and education must be relevant and sustainable
- **Attract, train, and retain talented cybersecurity professionals** – “Even the best cybersecurity tools in the world require talented people who know how to use them.” (OPM Breach report - Recommendations for Addressing IT Security and Data Protection Vulnerabilities)
- "I think that the lack of security professionals and the shortage of supply is one of the greatest threats facing the industry right now,"
- Security managers reported significant obstacles in implementing desired security projects due to lack of staff expertise (34.5%) and inadequate staffing (26.4%).





## Management Objectives

- **Certify the Workforce – INVEST IN YOUR PERSONNEL!!!**
  - Improved Cybersecurity posture
  - Provide a foundation of a professional workforce
  - Mechanism to “raise the bar” on cyber skills
- **Manage the Workforce**
  - Ability to place trained/capable personnel in cyber related jobs
  - Develop a career path – workforce management plan
- **Sustain the Workforce**
  - Elevate priority of Cybersecurity for training dollars
  - Enable personnel to hone Cybersecurity skills, keep current with latest technology, threats and vulnerabilities, tools and techniques
  - Create a pipeline for new talent (e.g. K-12 outreach)
- **Extend the Discipline**
  - Management at all levels who understand the impact of cybersecurity on mission accomplishment
  - Cybersecurity literacy for other critical workforces (e.g., procurement, HR etc.)



8/17/2015 7 Information Technology 7



## Training Opportunities

- NIST National Initiative for Cybersecurity Education (NICE)
  - NICE is a public-private partnership between government, academia, and the private sector
  - National initiative to address cybersecurity education, training, and workforce development
  - Cyber Education Map which plots schools offering cybersecurity programs across the country. Another way to both expand and improve the cybersecurity workforce is to bring a wide range of students into the educational pipeline that feeds industry and government needs
  - <http://www.cybereducationmap.org/map>
- Cybrary
  - Provides comprehensive IT and cyber security training options for underserved and disadvantaged people seeking to break into cyber security or move ahead in their current jobs
  - no-cost cyber security massive open online course (MOOC) provider
- Virtual Training Environments
  - <https://fedvte.usalearning.gov/>
- Vendor training and certification programs
- Service members have a myriad of opportunities from service schools to live cyber ranges to hone their skills



8/17/2015 8 Information Technology 8



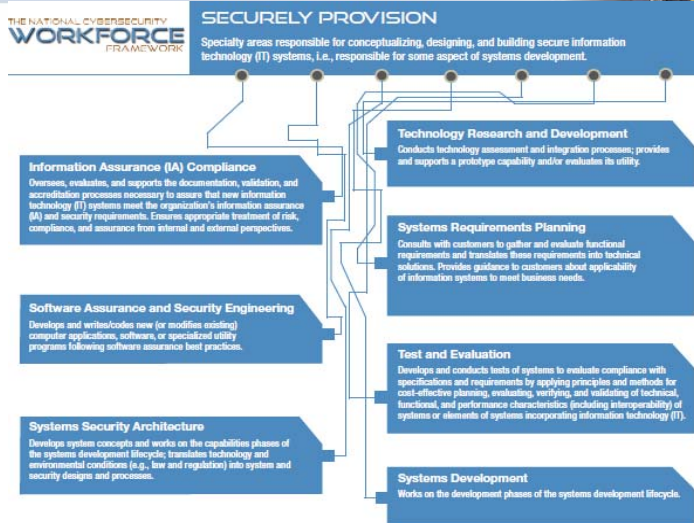
# NIST Framework

The NICE Cybersecurity Workforce Framework outlines 31 functional work specialties within seven Categories:

- Developed in collaboration with subject matter experts from government, non-profits, academia, and the private sector.
- Foundation for increasing the size and capability of the US cybersecurity workforce.
- National resource for employers, educators, trainers, and policy makers, providing a common cybersecurity lexicon.



# NIST Cybersecurity Framework






# NIST Cybersecurity Framework

**SECURELY PROVISION**
**INFORMATION ASSURANCE (IA) COMPLIANCE**

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

TASK ID	KSA	Statement
537		Develop methods to monitor and measure risk, compliance, and assurance efforts
548		Develop specifications to ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level
566		Draft statements of preliminary or residual security risks for system operation
691		Maintain information systems assurance and accreditation materials
696		Manage and approve Accreditation Packages (e.g., International Organization for Standardization/International Electrotechnical Commission [ISO/IEC] 15026-2)
710		Monitor and evaluate a system's compliance with information technology (IT) security, resilience, and dependability requirements
772		Perform validation steps, comparing actual results with expected results and analyze the differences to identify impact and risks
775		Plan and conduct security authorization reviews and assurance case development for initial installation of software applications, systems, and networks
798		Provide an accurate technical evaluation of the software application, system, or network, documenting the security posture, capabilities, and vulnerabilities against relevant information assurance (IA) compliances
827		Recommend new or revised security, resilience, and dependability measures based on the results of reviews
836		Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network
878		Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations
879		Verify that the software application/network/system accreditation and assurance documentation is current
936		Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers)
937		Inspect continuous monitoring results to confirm that the level of risk is within acceptable limits for the software application, network, or system




8/17/2015
Information Technology
11

# NIST Cybersecurity Framework

**SECURELY PROVISION**
**INFORMATION ASSURANCE (IA) COMPLIANCE**

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

TASK ID	KSA	Statement	Competency
19		Knowledge of computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities	Computer Network Defense
58		Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins	Information Systems/Network Security
63		Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
69		Knowledge of Risk Management Framework (RMF) requirements	Information Systems Security Certification
77		Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures, utilizing standards-based concepts and capabilities	Information Systems/Network Security
88		Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
121		Knowledge of structured analysis principles and methods	Logical Systems Design
126		Knowledge of systems diagnostic tools and fault identification techniques	Systems Testing and Evaluation
143		Knowledge of the organization's enterprise information technology (IT) goals and objectives	Enterprise Architecture
183		Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes	Information Assurance
203		Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance relative to the goals of the system	Information Technology Performance Assessment
942		Knowledge of the organization's core business/mission processes	Organizational Awareness



8/17/2015
Information Technology
12

## Cyber Workforce Goals

- Identify, classify our Cyber Workforce
  - Identify key stakeholders
  - Top down support
  - Obtain budget
  - Identify shadow IT elements
- Conduct Knowledge, Skills and Abilities Assessment
  - Identify training requirements
- Leverage our NC schools systems for talent
  - Engage early, recruit early

**MISSION: Recruit, Train and Retain**



## Questions?

Contact:  
Maria.S.Thompson@nc.gov

