


UNM Information Assurance Scholarship for Service (SFS) Program



What is Information Assurance?

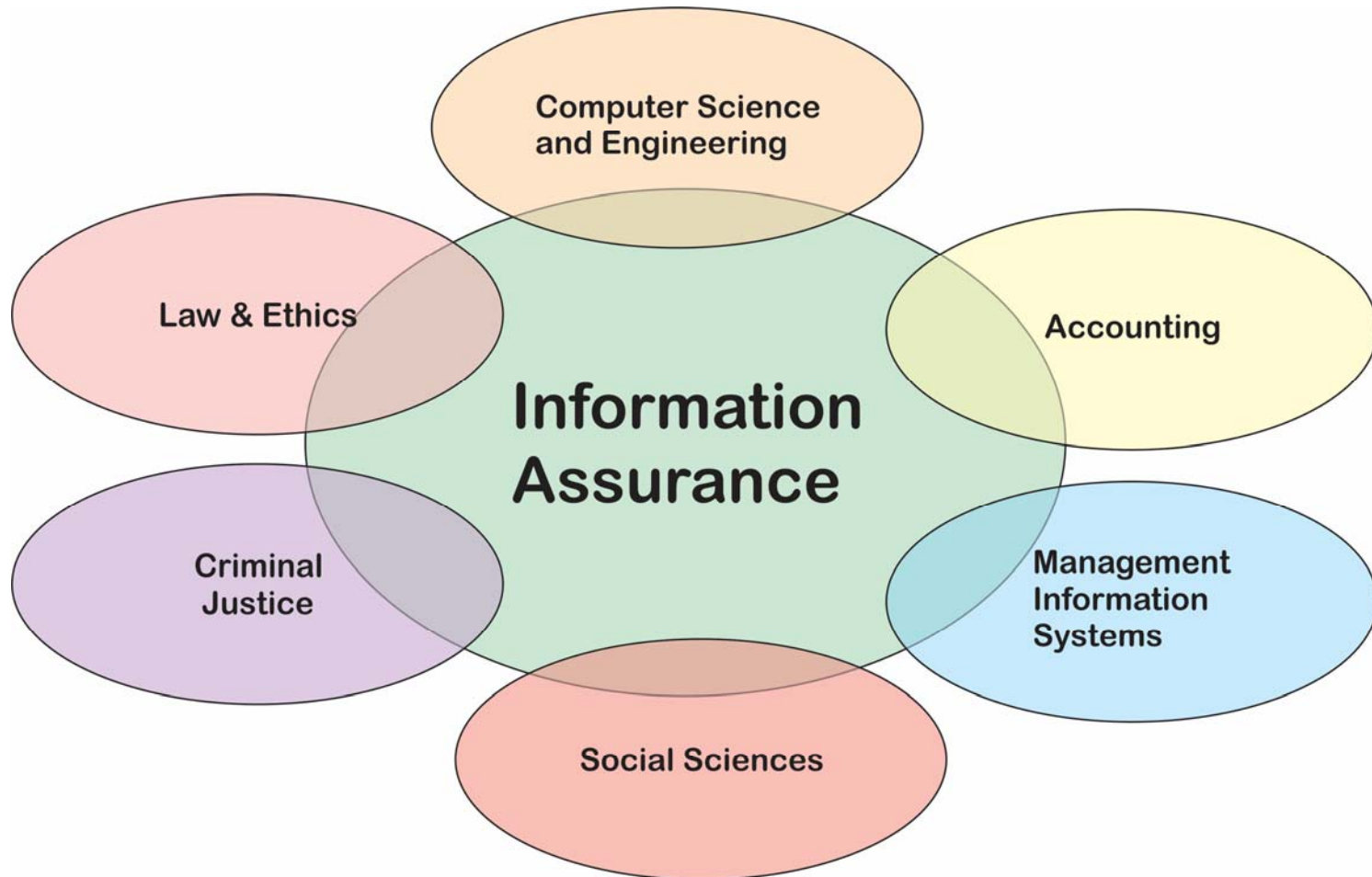
- Committee on National Security Systems (CNSS) defines information assurance (IA):



Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation

- Obvious subtopics:
 - Encryption
 - Network security
 - Intrusion detection
 - Secure coding practices
 - Digital forensics
- Not-so-obvious subtopics:
 - Fraud & forensic accounting
 - Security policy & implementation
 - Legal and privacy issues
 - Education & training

IA Overlap to Other Fields





Information Assurance at the University of New Mexico



UNM History

- Security courses and research within multiple departments since the 1990s – Engineering and Management schools
- UNM's Center for Information Assurance Research and Education (CIARE) established in 2006 in collaboration with national laboratories
- DHS/NSA designation as Center of Academic Excellence (CAE) in Information Assurance in 2007
- New Mexico regional computer forensics lab (RCFL) opens on UNM south campus in 2012
- Re-designation (CAE) in 2012 and CAE-R
- NSF Scholarship for Service grant in 2013



UNM – Current IA Programs

- Master of Accounting - IA concentration
 - 33 semester credit hours with 12-15 in IA
 - Graduates work primarily in fraud/forensic accounting, internal auditing, and public accounting
- Master of Computer Science
 - 33 semester credit hours
 - Cybersecurity emphasis available through multiple courses and research projects
- Master of Electrical & Computer Engineering
 - 33 semester credit hours
 - Cybersecurity emphasis available through multiple courses and research projects

UNM – Current IA Programs - Continued

- Master of Science (MS) in Information Systems and Assurance
 - Minimum 32 semester credit hours
 - No formal tracks – take courses in IA, MIS, or both
 - Study plans customized to student background and career goals
 - 4 management core courses required but waived for students with an undergraduate management degree
 - IS Security, database management, project management, and professional communications are required but waived for students with similar undergraduate coursework
 - Remaining courses taken from IS/IA electives
 - A thesis option is available

UNM IA SFS Program

- UNM was awarded a National Science Foundation grant to create the UNM Information Scholarship for Service (SFS) Program – 18 scholarships over 3 years
- Similar programs at a few dozen universities though only 3 are administered within management schools
- Students are funded to complete an IA-related Master's degree in exchange for accepting a job with the Federal Cybercorps

UNM IA SFS Program Summary

- Complete a Masters degree in IA at UNM following pre-approved study plan
- Full funding for three semesters
- Mandatory summer internship in Washington, D.C.
- Mandatory 2-years employment in Federal Cybercorps
- Must be a U.S. citizen and able to receive a security clearance

UNM IS SFS Per Student Funding

- Tuition and all fees
- Stipend - \$2083 per month
- Book allowance - \$500 per semester
- Travel to job fairs and conferences
- Health insurance reimbursement

Student Timeline

- Apply for scholarship by September (for January start) or by May (August start) – must also apply for Master's program
- Interview for scholarship
- Recipients notified in October or June
- Preparation during fall for January SFS job fair in Washington, D.C – find an internship
- Complete spring (or fall and spring) courses
- Complete internship in summer
- Complete remaining courses
- Attend January SFS job fair – find a Cybercorps placement
- Graduate and begin work in the Federal Cybercorps

UNM Center for IA Research & Education (CIARE)

- Focal point for research efforts on campus
- Meet & greet space for IA students
- Meeting space for external collaboration and outreach efforts
- IA computer labs

UNM CIARE – Research

- Digital Forensics
- Intrusion Detection
- Incident Response
- Malware
- Steganalysis
- Digital Rights Management
- Pen Testing and Assessments
- Corporate and Financial Fraud
- White and Red Collar Crime
- Social Engineering
- Internet Banking
- Identity Theft
- Virtualization

UNM CIARE – Outreach

- K-12 community support in cyber security (presentations, training, awareness) – Over 80 NM schools since 2007
- Information Security Assessments – Developed in partnership with NM DHS, 10 organizations served since 2009
- Fraud Prevention Audits – Service in support of non profit organizations in New Mexico
- Material expert presentations to community – Minimum of quarterly presentations on cyber security, fraud prevention and information security management

UNM CIARE – Partnerships

- FBI – NM Regional Computer Forensics Lab, actively engaged in research and internship collaborations
- Sandia National Laboratories - College Cyber Defenders Program with satellite office on campus dedicated to cyber security research and internships
- Los Alamos National Laboratories – Digital forensics, intrusion detection and incident response internships
- US Attorney’s Office, Secret Service and local law enforcement – fraud, forensic accounting and white collar crime research and internships
- NSA – Onsite research presentations and internships
- Industry – Various and growing



UNM CIARE – Students

- Background in technical areas including computer science, engineering, information technology, and accounting
- Actively engaged in community (K-12, InfoSec Assessments & Fraud Prevention Audits)
- Internships (NM RCFL, Sandia, LANL, US Attorney, Secret Service and local law enforcement agencies)
- Regularly participate in cyber security competitions
 - TracerFIRE (Sandia/LANL Forensics and Incident Response)
 - Computer and Network Vulnerability Assessment Simulation (CANVAS, NSA and Air Force Academy)
 - National Collegiate Cyber Defense Competition (CCDC)

UNM CIARE – Funding

- NSA/DHS – Scholarship for Service \$1.67 M
- Dell - \$220,000 for design and development of the advanced virtual cloud lab infrastructure (VLAB)
- UNM/State of NM - \$150,000 (yearly for 10 years) in support of the NM RCFL
- CitiCards - \$5,000 for small business fraud prevention training seminars

IA Centers of Academic Excellence (CAE)

- Joint designation by National Security Agency (NSA) and the Department of Homeland Security (DHS)
- Higher education institutions must meet minimum standards for IA-related curriculum, resources, research
 - **CAE/2Y** - National Centers of Academic Excellence in Information Assurance 2-Year Education
 - **CAE/IAE**- National Centers of Academic Excellence in Information Assurance Education
 - **CAE/R** - National Centers of Academic Excellence in Information Assurance Research
- Designated institutions are:
 - Eligible to apply for targeted grants
 - Targeted for Federal Cybercorps hires
- Currently 181 designated institutions

Curriculum Standards

- Until this year, CAE curriculum standards were based on CNSS training standards:

| Standard | Description | Last Revised |
|----------|-------------------------------------------------------------------------------------|--------------|
| 4011 | National Training Standard for Information Systems Security (INFOSEC) Professionals | 1994 |
| 4012 | National Information Assurance Training Standard for Senior Systems Managers | 2004 |
| 4013 | National Information Assurance Training Standard For System Administrators | 2004 |
| 4014 | Information Assurance Training Standard for Information Systems Security Officers | 2004 |
| 4015 | National Training Standard for Systems Certifiers | 2000 |
| 4016 | National Information Assurance Training Standard For Risk Analysts | 2005 |

Curriculum Standards Update

- Multiple initiatives are in progress to update obsolete standards:
 - NSA-led effort to define curriculum standards for *cyber-operations*
 - NSA/DHS effort to update *IA curriculum standards* for CAE designation
 - *National Initiative for Cybersecurity Education*
- There is overlap and competition among these efforts

Cyber-operations Standards

- NSA and (to a lesser extent) DOD and DHS have unique requirements for personnel engaged in cutting-edge attack and defense
 - Greater reliance on CS, engineering, and math skills
 - Rapidly changing environment less amenable to “canned” solutions
 - Greater need for research skills
- Cyber-operations standards reflect their unique needs
- Standards resemble “old-fashioned” programs in computer science and engineering
 - Breadth vs. depth
 - Theory vs. application
- Only a handful of schools have such a curriculum – **Why?**

Updated CAE Standards

- Content and structure both updated:
 - Modernized technology and related issues (for example, social networking, handheld devices, and ubiquitous wireless communication)
 - Modernized curriculum constructs (for example, knowledge units with well-defined learning objectives)
- Content has been broadened to reflect the breadth of IA rather than the narrowness of computer/network security
 - Result should be a more diversity in participating institutions, programs, and academic departments
- Substantial room for institutions and programs to define unique niches, for example:
 - White collar crime
 - Security administration and compliance
 - Behavioral aspects of cybercrime and risk mitigation

NICE

- National Initiative for Cybersecurity Education (NICE)
 - *“NICE is a national campaign designed to improve the cyber behavior, skills, and knowledge of every segment of the population, enabling a safer cyberspace”*
- A key component is the National Cybersecurity Workforce Framework
 - Targeted more to workforce development/training but does reflect the breadth of IA

National Cybersecurity Workforce Framework

