Introduction

The social and economic well being of the nation and Pacific Northwest region is more dependent than ever on information infrastructure managed by computer software systems and networks. We are connected in ways we have never been before, are more dependent upon our networked infrastructure than ever before, and are increasing our dependence on ever more complex networked infrastructures. New protections against mobile program code attacks - worms, virus, et al - and denial of service threats are required, in addition to age-old protections like encryption, backup & recovery, system access control, contingency operations, and disaster recovery.

The challenges of Information Assurance are not going to be solved easily, quickly, or independently. Solutions will require new research, new capabilities, new products and services, a spectrum of broadly and uniquely educated professionals, an increasingly aware public, and much more innovative and broad-ranging forms of collaboration. International commerce, military defense, and network-based software development are all major industries in the state of Washington. As such, Washington is both vulnerable to disruption, as well as home to a spectrum of professional talent and organizations that can be well served by the presence of a national center of excellence.

Vision

The Center will be an axis point for Pacific Northwest research, education, industry and government, providing innovation and leadership in the protection of critical public and private information infrastructures, and well-educated information assurance and cybersecurity at all professional levels.

Mission

The mission of the Center will be to provide a forum for the collaboration of professors, professionals, industries, and students. It will identify, address, and promote visions and solutions for issues of information assurance and cybersecurity. The Center will produce and be a catalyst for research, invention, innovation, education, public awareness, entrepreneurship, and economic growth in the state of Washington. Its efforts will help to sustain the vitality of existing industries, as well as to attract and develop new industries. The Center will emphasize participation of underrepresented groups, especially women and people of color, in secure computing and data integrity, and promote the practice of emerging security standards.
Goals

The Center’s focus will promote the following activities:

- Research by and for collaborating universities, colleges, industries, and government units and individuals;
- A breadth of offerings of diverse and complementary academic university programs of study at both undergraduate & graduate levels;
- Technical certification and training programs provided by community and technical colleges;
- Workshops, conferences, and lecture series provided by and for practicing security professionals through professional continuing education units;
- Unique shared facilities including computer security forensic laboratories;
- Funding to attract and retain outstanding faculty and research expertise;
- Funding for student scholarships, particularly targeting underrepresented groups;
- “Scholarship for Service” programs that fund education for and with commitment for employment after graduation;
- Internships that match students with professionals, organizations, and innovative projects in the area;
- State of the art repository of information assurance & cybersecurity resources;
- Entrepreneurship and incubator collaboration and support,
- Consulting services in leading edge areas of intrusion response, computer forensics, computer crime litigation, etc.;
- Joint Development Partnerships with local companies producing security related software and hardware products; and
- Demonstration of best practices in information assurance & cybersecurity.

The Center will provide and/or encourage education, research, and support in a breadth of areas of information assurance and cybersecurity, including:

- Security Risk Assessment and Management
- Policies, Laws, and Rights Management
- Security Awareness Issues and Processes
- Security Tools and Applications
- Trusted Interactions and Data Gathering
- Assurable Software and Architectures
- Network and Enclave Security
- Incident Detection and Response
- Incident Forensics
- Cryptology

Principle Center Participants:

The Center will attract a diverse set of colleagues including the following founding participants:

- Hilda Blanco        Professor, Urban Design & Planning Studies
- Larry Crum          Professor, Computing & Software Systems
- Sergio Davalos      Assistant Professor, Milgard School of Business
- David Dittrich      Research, Information School
                       Senior Security Engineer, Computing & Communications
- Andrew Fry          Lecturer, Computing & Software Systems
- Steve Hanks (Director) Professor, Computing & Software Systems
                       Assistant Director for Industry Relations, UWT Inst of Tech
Industry Partners

There are anticipated to be many industrial collaborators with the Center. Initially, they are likely to include:

- Boeing
- Microsoft
- Intel
- Port of Tacoma
- Sagem Morpho
- Pacific Northwest National Laboratories
- Topia Technologies
- Real Networks
- Keyport and Bangor Naval Bases
- Ft Lewis Army Base
- Advanced Interactive Systems
- Prepared Response
- Mobilisa
- Ascentry Technologies
- ID Micro
- Concur

Strategy

Several key laboratories currently exist or are now being created. They provide ideal initial environments for research, teaching, and industry projects. For example, Dr. Radha Poovendran’s Network Security Lab in the Electrical Engineering Building has active funded research projects and supports graduate students. The UWT Institute of Technology’s Information Assurance & Cybersecurity laboratory will be operational by Spring quarter 2004 and will move its security-oriented research projects into it. The Information School has research space allocated for forensic study and projects. The new Morken Center at PLU will house a network security laboratory combining resources from the Departments of Computer Science & Engineering.
Science & Engineering, Business, and Mathematics. All of these spaces are expected to contribute to the environment of the proposed Center, and all are expected to benefit from its existence.

An early priority for the Center is to obtain recognition as one of the official National Security Agency (NSA) Centers of Academic Excellence in Information Assurance Education. This designation creates opportunities for special government support in grants, scholarships, and internships, as well as unique opportunities to work collaboratively with the other such centers around the country. There are fifty such Centers now recognized by NSA, but only the Naval Postgraduate School, Stanford, UC Davis, and Portland State are on the West Coast. Most are concentrated in the east and particularly the northeast. The NSA desires to have centers strategically distributed geographically. The next deadline for consideration for NSA Center recognition is December 10, 2003. The center will submit a proposal for that consideration. The criteria are listed in the Appendix.

The Center will collaborate with the Pacific Northwest Information Assurance & Security Consortium (IASC), an association of industry, government, and education representatives that has a vision of insuring that the Pacific Northwest information structure and practice is the safest and most secure in the world. It was organized with the leadership of Boeing and Congressman Dicks.

The Center will also collaborate with the Regional Alliance for Infrastructure and Network Security (RAINS), which is a public/private partnership whose purpose is to accelerate the development and deployment of innovative new technologies for cyber and homeland security. RAINS is a complementary organization to the IASC.
Appendix

Centers Of Academic Excellence in
Information Assurance Education
Graduate & Undergraduate
Criteria for Measurement
Point System Qualification

1. Provide evidence of partnerships in Information Assurance education with historically underrepresented colleges and universities (HUCU), 2-year community colleges and technical schools. (10-15 points)

2. The academic program demonstrates Information Assurance is not treated as a separate discipline, but as a multidisciplinary science with the body of Information Assurance knowledge incorporated into various disciplines. (20-30 points)

3. The academic program demonstrates how the university encourages the practice of Information Assurance, not merely that Information Assurance is taught. (15-25 points)

4. The academic program encourages research in Information Assurance. (15-35 points)

5. The Information Assurance curriculum reaches beyond the normal geographic borders of the university. (15-50 points)

6. It is clearly demonstrated that the faculty is active in Information Assurance practice and research, and contributes to Information Assurance literature. Substantiate depth and length of faculty expertise through submission of biographies. (2-30 points)

7. The university library and reference systems/materials and/or the Information Assurance Center maintain state of the art Information Assurance resources. (20-30 points)

8. Academic program, within a nationally accredited 4-year college or graduate-level university, has declared concentrations. Identify the courses required for each concentration, provide syllabus, enrollment data for current academic year (not projected) and actual matriculation data (not projected) for the past two academic years. (30-150 points)

9. The university has a declared center for Information Assurance education or a center for Information Assurance research from which Information Assurance curriculum is emerging. The center may be school, or university-based. (35-50 points)

10. University Information Assurance faculty consists of more than one individual. Includes shared and cross-departmental appointments for part-time and adjunct faculty. This may include institutional agreements for cooperative use/exchange of adjunct faculty from/between universities. (30-100 points)

Total Points: 210-515 (210 required to qualify)