



“Don’t be left out in the cold”

A Test bed Internet for the research, design, evaluation, and testing of security solutions.

For more information see [www.iac.iastate.edu/iseage](http://www.iac.iastate.edu/iseage) or contact:

Dr. Doug Jacobson  
Director: ISU Information Assurance Center  
2419 Coover Hall  
Iowa State University  
Ames, IA 50011  
Tel: 515-294-8307  
Fax: 515-294-8432  
[dougj@iastate.edu](mailto:dougj@iastate.edu)

## Project Overview

This paper describes an initiative to create an **Internet-Scale Event and Attack Generation Environment** (ISEAGE) (pronounced “ice age”) at Iowa State University. ISEAGE will be a first of its kind facility in a public university dedicated to creating a virtual Internet for the purpose of researching, designing, and testing cyber defense mechanisms as well as analysis of cyber attacks. Unlike computer-based simulations, real attacks will be played out against real equipment. Researchers and vendors are working hard to provide products and services to help defend against cyber attacks, but users of these technologies often do not have any mechanisms to test or even try out these defenses. Law enforcement agencies and forensics analysts have no way to replay attacks or recreate a cyber crime scene. ISEAGE will provide a mechanism to help solve cyber crime. The ISEAGE facility will provide a controlled environment where real world attacks can be played out against different configurations of equipment. ISEAGE will contain a vast warehouse of attack tools that will be able to simulate point-to-point and distributed attacks. The creation of ISEAGE will represent a new paradigm in the area of security research, cyber forensics, and will enable new and innovative research needed to solve the current security problems facing the world today.

## Problems to be Addressed

Information security has become a critical concern of government, law enforcement, and industry. Numerous groups have independently called for more and higher quality research and education efforts in computer security. During the first computer security education workshop (1997), sponsored by the National Security Agency and attended by industry and government agencies, there was a clear call to action for universities to create programs in information security. According to the President's 1998 Commission on Critical Infrastructure report, computer security is of prime importance to protecting the national communication infrastructure, and the report recommends increasing the education efforts in computer security. Additionally, Tom Ridge, secretary of the U.S. Department of Homeland Security, stated (Northern Virginia Technology Council, April 2003) “When it comes to security, you must be more than partners, you must be leaders. We think that the lesson learned from Y2K and 9/11 should be applied and not forgotten. This will not be a cost-free arrangement, but the cost of doing little or nothing will be much higher.” Ridge also called for the technology business people in attendance to do more to protect the U.S. technology infrastructure, noting that private companies control 85 percent of the nation’s cyber resources.

According to the Department of Homeland Security “Critical infrastructures supply us with the simple conveniences of every day life - turning on a light, using a telephone, or logging on a computer - as well as the goods and services Americans need to survive.” These conveniences and services provide the backbone of the U.S. economy. The USA Patriot Act defines critical infrastructures as *those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economy security, national public health or safety, or combination of those matters.* Protecting America's infrastructure and key assets is a formidable challenge.

The Department of Homeland Security has identified a set of critical infrastructures that the nation relies upon, ranging from energy, transportation, banking, food, etc. The cyber infrastructure has been list as a critical asset and needs to be protected. However an argument can be made that with the exception of energy no other critical asset is as critical to the operation of every other critical sector. An even the energy sector can not operation today without the cyber infrastructure. Given the importance of the cyber infrastructure to the security of the nation it is logical that homeland security be one of the areas of focus for ISEAGE.

Due to the interdependencies of the nation's infrastructure, securing that infrastructure requires the coordination of many different stakeholders. Research efforts and proposed solutions can no longer be disjointed and must focus on the overall problem which may involve expertise from a diverse group.

According to the recently published report by the Presidents Information Technology Advisory Committee

([http://www.nitrd.gov/pitac/reports/20050301\\_cybersecurity/cybersecurity.pdf](http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf))

“The Nation’s IT infrastructure has undergone a dramatic transformation over the last decade. Explosive growth in the use of networks to connect various IT systems has made it relatively easy to obtain information, to communicate, and to control these systems across great distances. Because of the tremendous productivity gains and new capabilities enabled by these networked systems, they have been incorporated into a vast number of civilian applications, including education, commerce, science and engineering, and entertainment. They have also been incorporated into virtually every sector of the Nation’s critical infrastructure – including communications, utilities, finance, transportation, law enforcement, and defense. Indeed, these sectors are now critically reliant on the underlying IT infrastructure.

At the same time, this revolution in connectivity has also increased the potential of those who would do harm, giving them the capability to do so from afar while armed with only a computer and the knowledge needed to identify and exploit vulnerabilities. Today, it is possible for a malicious agent to penetrate millions of computers around the world in a matter of minutes, exploiting those machines to attack the Nation’s critical infrastructure, penetrate sensitive systems, or steal valuable data. The growth in the number of attacks matches the tremendous growth in connectivity, and dealing with these attacks now costs the Nation billions of dollars annually. Moreover, we are rapidly losing ground to those who do harm, as is indicated by the steadily mounting numbers of compromised networks and resulting financial losses.

Although the large costs associated with cyber insecurity have only recently become manifest, the Nation’s cyber security problems have been building for many years and will plague us for many years to come. They derive from a decades-long failure to develop the security protocols and practices needed to protect the Nation’s IT infrastructure, and to adequately train and grow the numbers of experts needed to employ those mechanisms effectively. The short term patches and fixes that are deployed today can be useful in response to isolated vulnerabilities, but they do not adequately address the core problems. Rather, fundamental, long-term research is required to develop

entirely new approaches to cyber security. It is imperative that we take action before the situation worsens and the cost of inaction becomes even greater.”

In addition the report goes on to report several findings and recommendation including finding 2:

“The Nation’s cyber security research community is too small to adequately support the cyber security research and education programs necessary to protect the United States.

#### Recommendation 2

The Federal government should intensify its efforts to promote recruitment and retention of cyber security researchers and students at research universities, with a goal of at least doubling the size of the civilian cyber security fundamental research community by the end of the decade. In particular, the Federal government should increase and stabilize the funding for fundamental research in civilian cyber security, and should support programs that enable researchers to move into cyber security research from other fields.”

The Committee analyzed more than 30 reports on cyber security R&D to identify 10 priority areas for increased emphasis. These areas are of paramount importance. Without significant advances in research in these areas, the Nation will not be able to secure its IT infrastructure. Cyber Security research priority number eight is “Modeling and Testbeds for New Technologies:”

“One of the barriers to the rapid development of new cyber security products is the paucity of realistic models and testbeds available for exercising the latest technologies in a real-world environment. Some Internet modeling research has been conducted, but it has been rudimentary and has had little impact in practice. The problem is challenging because of the Internet’s scale and complexity. Additionally, existing data on the Internet’s workings are limited and typically confidential. Some Federal programs have been established recently, but a significantly larger and more sophisticated effort is needed if useful models and testbeds are ever to become a reality. Research subtopics include:

- System simulation environments
- Validating simulations involving millions of nodes
- Gathering and synthesizing very large amounts of data
- Designing a testbed that preserves the confidentiality of data”

In response to these demands, the faculty from several departments of Iowa State University created the **Information Assurance Center (IAC)** as a structure to provide a focal point for research and teaching in computer security. The center is an interdisciplinary body, drawing faculty from technology-based disciplines, the liberal arts and sciences, and education. By bringing faculty members from these disciplines together, ISU is able to respond to the needs of students and the priorities of different sectors in government, business, and society. We currently have over 30 faculty members affiliated with the ISU IAC. Through the leadership of

the faculty, the IAC has grown into a national leader in computer security education. The following are its recent accomplishments:

- It has become one of the largest and oldest programs in the country.
- It is designated as a charter Center of Excellence in Information Assurance (COE) by the National Security Agency. The goal of the NSA COE initiative is "to reduce vulnerability in our National Information Infrastructure by promoting higher education in information assurance, and producing a growing number of professionals with Information Assurance expertise in various disciplines."
- The faculty of the IAC participated in a grant initiative of the federal government and successfully received funding from the National Science Foundation in 2001 to train "Cyber-corps" for federal agencies.
- The faculty created an interdisciplinary Masters Degree in Information Assurance.
- The faculty created a Graduate Certificate in Information Assurance to meet the needs of professionals wishing to enhance their education.

Given its initial success, the IAC proposes to take the next step to expand its capabilities by building a world class testbed environment (ISEAGE).

As discussed in the report from the NSF workshop on network research testbeds the need for testbed networks is well documented. We believe this is especially true in the area of security research, where too often security research is based on either data from the internet directly or from artificial data. Either way this can lead to results that are hard to recreate or may not apply to the real world. By recreating the internet for the purpose of launching controlled attacks in the presence of known background data the investigators are confident that higher quality research results will be obtained. ISEAGE will provide this environment and will facilitate a level of research well beyond the current state of the art. Another problem that often faces security researchers and companies producing security technology is the ability to test their theories and solutions in a real life environment. This is often done by trying to convince an organization to beta test a new concept in their environment. This leads to many potential problems for both the researchers and the end users. ISEAGE will provide a place to evaluate the effectiveness of security products by being able to re-create attacks. Another problem with the way security is handled is that we are always in a defense mode waiting for the next attack and hoping that are technology will hold back the attack. In the case of the nation's critical infrastructure the current method of protection is to try to "break-in" to the live system every so often. We have been talking with the state of Iowa about using ISEAGE to constantly attack a replicate of the critical infrastructure with the goal of finding the problem before it happens to the live system.

There have been several successful network testbeds, but ISEAGE is designed specifically for use in security research and offers many advantages over a conventional network testbed. The primary advantage is the tool set that will be designed for ISEAGE.

## **Goals and objectives**

The goal of ISEAGE is to provide a world class research and education facility to enhance the current state of the art in information assurance. This one of kind facility will be the catalyst for bringing together top researchers from several disciplines for a common goal of making computing safer. The ISEAGE will provide an integrated environment to work on synergistic research projects in information assurance and to solve the problems facing industry, government, and law enforcement. The research areas in information assurance at Iowa State

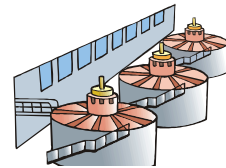
University deal with overlapping problems and can benefit from a common laboratory. For example, the group working in intrusion detection and the group working in survivable networks often utilize the same attack data and are concerned about the same types of attacks. The ISEAGE will be a critical element needed to elevate the research efforts and to help provide solutions to these complex problems.

We have already had numerous discussions with government agencies, law enforcement, business, and industry about the potential benefits of the ISEAGE. The following provides a summary of the potential impact and goals of the ISEAGE project on various groups:

- **Critical Infrastructure protection:**

**Issues:**

According to the Department of Homeland Security “Critical infrastructures supply us with the simple conveniences of every day life - turning on a light, using a telephone, or logging on a computer - as well as the goods and services Americans need to survive.” These conveniences and services provide the backbone of the U.S. economy.



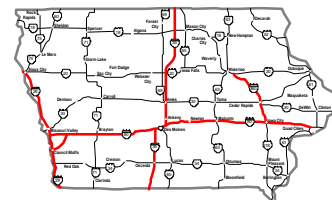
The USA Patriot Act defines critical infrastructures as *those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economy security, national public health or safety, or combination of those matters.* Protecting America's infrastructure and key assets is a formidable challenge.

The Department of Homeland Security has identified a set of critical infrastructures that the nation relies upon, ranging from energy, transportation, banking, food, etc. The cyber infrastructure has been list as a critical asset and needs to be protected. However an argument can be made that with the exception of energy no other critical asset is as critical to the operation of every other critical sector. An even the energy sector can not operation today without the cyber infrastructure. 85% of the cyber infrastructure is owned by the private sector. Given the importance of the cyber infrastructure to the security of the nation it is logical that homeland security be one of the focuses of the ISEAGE project. This infrastructure can be federal, state, local or corporate.

Another problem is providing realistic environments to train for cyber attacks or cyber failures. Most table top exercises do not provide an environment that directly tests security plans under adverse conditions.

**How to use ISEAGE:**

The ISEAGE can be used to recreate critical components of an infrastructure on an ongoing basis. These live models of the infrastructure will be subjected to constant attacks to probe for weaknesses and to try the newest attacks before they become a threat to the actual infrastructure. Any detected weakness will be used to strengthen the actual infrastructure. The goal would be to develop algorithms and methods to harden the networks and computers used to support the critical infrastructure. ISEAGE has also been written into the State of Iowa Homeland Security Plan as a critical resource for securing the state's critical infrastructure. We have started a project to model the state of Iowa network. This type of model will



operate at two levels, first we will be able to model the infrastructure at the GIS level to be used for business continuity and interdependency modeling. In this type of model, we will be able to model the entire state network and look at the impact of faults at any location, whether man made or natural. The other model would be at the system level where critical state assets are modeled and then attacks are launched against the assets. For example a state wide authentication system could be modeled and attacked. When coupled with the first model we can examine both system and infrastructure outages. Lessons learned from the research will be exported to other states. ISEAGE will also provide an environment for table top training exercises as discussed in the section on education, training, and outreach.

- **End-users of security:**

**Issues:**

End users of security are often forced to deploy technology without field-testing. In addition end-users often have the same infrastructure issues that were outlined above. End users also do not have a method to train on new technologies in a realistic setting.



**How to use ISEAGE:**

The ISEAGE facility will provide a place for to test out security configurations prior to deployment and to try equipment and configurations from different vendors. Many of the distributed attacks rely on the inherent weaknesses in the end user systems. By looking at the security of end user systems we can develop new methods to provide increased security for all systems. ISEAGE can be used in a couple of different configurations that would be beneficial to end-users. The first configuration is where they are concerned about the security of a single location and the internet is treated as a single attack point. In this scenario ISEAGE would be configured to provide what looks like the companies ISP connection and would generate traffic that would mimic what they see in their own environment. Connected to ISEAGE would be a duplication of the equipment that is used by the end-user or equipment they are wishing to evaluate. Attacks would then be launched against the end-users model environment. This can also be used as a training environment (see the section on training) for the end-user employees.

The second configuration would be very similar to the infrastructure scenario where ISEAGE would be used to model an end-user's infrastructure (either internal or between remote sites). As in the first configuration equipment would be connected to ISEAGE and attacks would be launched against both the equipment and the infrastructure. ISEAGE will also provide an environment for table top training exercises as discussed in the section on education, training, and outreach.

- **Developers of security:**

**Issues:**

Developers of new security devices often find it difficult to test new ideas and methods in a controlled environment. In addition having an independent facility that can provide a testing environment will provide additional information needed for product development.



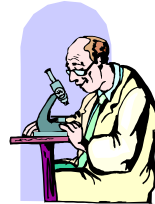
**How to use ISEAGE:**

The ISEAGE facility will provide a test environment for developers to deploy versions of their products. We envision working on jointly funded research projects to create new methods, processes, and algorithms to provide security. ISEAGE can also be used by security vendors to showcase new security products

- **Academic and industrial Researchers:**

**Issues:**

Just like security vendors, researchers often find it difficult to recreate a realistic environment that will provide a testbed to try out new ideas.



**How to use ISEAGE:**

The ISEAGE facility will be designed to provide an excellent environment to conduct state of the art research in computer security and security tool development. Iowa State University has over 30 faculty members involved in security and has received funding for a NSF Industry/University Cooperative Research Center (I/U CRC) that will focus on information protection. Members of the center will have access to ISEAGE for research projects. Additional information on the I/U CRC Center for Information Protection is provided at the end of this document.

- **Forensics and Law enforcement agencies:**

**Issues:**

Law enforcement agencies need access to a laboratory to experiment with the tools used by the attackers and to look at methods to trace back attacks and new tools to aid in the detection, apprehension, and conviction of attackers and other cyber criminals. In addition they need a facility that can be used for training.



**How to use ISEAGE:**

The IAC faculty members have worked with several local law enforcement agencies to provide computer forensics support, advice, and training. The ISEAGE can be used to create new tools and methods to support law enforcement. Iowa State University's Department of Public Safety (DPS), Information Assurance Center (IAC), and Midwest Forensics Resource Center (MFRC) have coordinated their existing resources to establish a computer crime investigation effort. The participants include the DPS's computer crime investigator, senior faculty and students from the IAC, researchers from the MFRC, and MFRC crime laboratory partners. The effort will not only help law enforcement but will provide a resource for business and industry if they experience a cyber incident. ISEAGE will be used to support the cyber crime lab.

- **Education, training, and Outreach:**

**Issues:**

There is a need for education and training at all level (k-12 through college to adult education). There is also a need to provide training for security staff on new equipment and to perform live fire drills. As discussed in for the infrastructure there is a need for realistic table top exercises.



**How to use ISEAGE:**

Iowa State University offers several courses in information assurance and networking that will greatly benefit from access to ISEAGE. We will also use ISEAGE for training for security professionals and to provide a real-world environment to train against attacks. It will also be used as a training facility for cyber forensics, giving investigators the ability to examine large cyber attacks in real time. We have already run a cyber defense competition where students defended networks against local IT security personal. We have held a wireless hacking demonstration for the local InfraGard chapter where the participants’ setup wireless access points and then used common attack tools to compromise the network. We are planning additional cyber defense competitions where local IT professionals setup and defend networks against each other. ISEAGE will also be used for table top exercises for both local businesses and state and local government.

**Implementation Plan**

ISEAGE in itself is a research project and will require the development of new software. The table below shows the timeline for the completion of ISEAGE. The implementation plan document provides more detail on how ISEAGE is built and the software tools need to fully deploy ISEAGE.

Item	Year 1				Year 2				Year 3			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Acquire Core switch and tap point												
Cyber Crime Lab												
Tool design and implementation												
Working prototype												
Scale the lab												
Documentation and users manual												
Forensics work												
Research project usage												

To date ISEAGE has received over \$500,000 in funding with another \$700,000 anticipated by August 2005. We are now in year 2 of the project.

There are two primary sets of deliverables from this project. The first set will be the tools designed to support ISEAGE. We will make the tools and the source code available to the research community. The research used in the design and creation of several of the tools will result in a masters thesis and publications. Many of the tools can be used in a small network environment to test a particular aspect of security and will prove useful to the general research community. The second set of deliverables is the research results for the projects enabled by the creation of ISEAGE and the usage of ISEAGE for forensics work and support of Business and industry. These results will be disseminated though journal publications, conference papers, technical reports and usage data. We will also create documentation on the overall design of ICEAGE and will make ISEAGE available to the community.

## **Evaluation plans, Outcomes, and Effectiveness of the Program**

There are numerous metrics for measuring the success of ISEAGE. The four dominant metrics are tools usage, ISEAGE usage, increases in funding, increases in scholarship. Many of the tools will be able to be used in smaller lab environments and even as stand alone devices. As mentioned before, we plan on making the tools available to the research community and a measure of success will be based on the level of adoption for the tools. One of the primary measures of success will be the overall usage of ISEAGE. Since the ISEAGE is being designed to handle many different types of security problems and many different users we anticipate heavy use. We anticipate that once ISEAGE is fully implemented the facility will be used continuously. Many of the activities are synergistic and can coexist. The last two metrics are traditional metrics used to measure the success of any research project. The difference in the case of ISEAGE is that we will measure success based on the funding of both research projects and the ongoing funding of ISEAGE. ISEAGE will also increase the level of scholarly publications through the increase in research and through publications based on the research into the building of ISEAGE. We believe that when ISEAGE is completed that it will be a model for security testbed networks in academia, industry, and certification organizations.

### **Sustainability:**

One key aspect to any testbed network is how to keep it running and how to fund additional equipment and upgrades. There have been numerous groups interested in ISEAGE including state government, private industry, and law enforcement. We will be able to develop a plan to keep the lab operational. Several key components of the operational plan are listed below.

The operation of ISEAGE will be managed by the Iowa State University Information Assurance Center which reports to the vice provost of research. This allows ISEAGE to become a university resource and should reduce any potential friction between departments and colleges over ownership.

Ongoing maintenance of the lab during the startup phase will be handled by a combination of time from the current computer support staff and graduate students. We also have several undergraduate students who work on research projects and in the current lab. We often have these students involved with setting up experiments and working on projects.

The seed funding will be used to help secure space and to fund some of the initial equipment needed to bring in additional funding for the ISEAGE, through equipment donations and other state and local funding sources. Due to the creation of the ISEAGE we envision an increase in external funding from government and private sources. When appropriate costs of lab upkeep and enhancement will be included in the proposals.

We will develop a charge back system to allow private industry to use ISEAGE which will help fund the support staff needed to keep the lab running. As we see an increase in external use that will provide an increase in funding this will allow an increase in staff support.

## Involvement

There are several way to become involved with ISEAGE depend on your goals. The table below show how an organization can become involved based on their goals

Usage	Options
<ul style="list-style-type: none"> <li>• Research Projects</li> <li>• Critical Infrastructure</li> </ul>	<ul style="list-style-type: none"> <li>• If you have a research project that would benefit from the usage of ISEAGE and would like to combine your resources with other companies to solve complex projects then join the Center for Information Protection <a href="http://www.iac.iastate.edu/cip">www.iac.iastate.edu/cip</a> Members of CIP receive access to ISEAGE through the research projects funded by the membership fees. They also receive additional access to ISEAGE for other projects. Members of CIP are part of an advisor board that sets the research agenda for CIP and will have input into ISEAGE.</li> <li>• If you have a specific project you can fund a research project directly with the ISU IAC</li> </ul>
<p>Product Testing, evaluation, and design.</p> <p>Training</p>	<p>Use ISEAGE by either:</p> <ul style="list-style-type: none"> <li>• Donations of equipment or money. Companies that donate equipment or funds to ISEAGE will receive access to ISEAGE based on the donation level. Companies that make major donations will also become members of the industrial advisory board.</li> <li>• Sponsorship allows a company to play a major role in ISEAGE by becoming part of the advisory board. Sponsors will also receive access to ISEAGE.</li> <li>• Hourly fee based access are for companies that have a small project that requires access to ISEAGE</li> </ul> <p>We offer several different venues to become involved in training depending on your goals and needs</p> <ul style="list-style-type: none"> <li>• We offer training exercises during the year, while many are closed to a specific group, we antcipant offering some open events.</li> <li>• Your organization can request a training event. This can range from a few hours to a few days depending on your goals.</li> <li>• If you are a security vendor you may wish to provide equipment for our training exercises.</li> <li>• If you are a vendor or reseller you can use ISEAGE to offer training on your equipment to potential customers.</li> </ul>

There are numerous synergistic activities between ISEAGE and other projects undertaken by the IAC. The project most directly associated with ISEAGE is the Center for Information Protection.

### **NSF I/U CRC Center for Information Protection (CIP)**

In response to these demands ISU has formed a partnership with New Jersey Institute of Technology to develop a NSF Industry/University Cooperative Research Center with a focus on information assurance called the Center for Information Protection. Given the initial success of the participating universities, we propose to take the next step to strengthen our combined capacity to serve the research and application needs of government and business. Information Assurance is the primary research focus of this project. Information assurance is commonly defined by the four goals of security, namely, "Confidentiality, Integrity, Availability, and Policy". By its very nature information assurance is a multidisciplinary research area. While most universities who perform research in computer security focus solely on the technical issues, we are proposing a truly multidisciplinary effort with faculty from multiple departments at multiple universities. It is this combination of technology, business issues, policy concerns, leadership, and ethics that make our program unique and will allow us to produce highly qualified researchers and educators.

**The Purpose of the Center for Information Protection** is to research and validate the means and methods necessary to improve the overall assurance posture of this nation's cyber infrastructure. To this end, the CIP will partner with industries that provide security solutions as well as industries that use these solutions in the creation of an overall security perimeter designed to protect data and information assets critical to their industry.

**The Vision of the Center for Information Protection** is to bring together, through research, the solution providers and the organizations that rely on the cyber infrastructure to identify and solve the complex security problems facing organizations. The center will be the communication mediator for the exchange of ideas and to identify common problems and concerns facing the cyber infrastructure.

**The Goals of the Center for Information Protection** are to (1) assist industry in its internal research and development by partnering industrial and faculty researchers; (2) improve the training and education of employees in Information Assurance; (3) provide a common repository for all CIP members that contains information assurance research results, relevant literature, and other resources that can be shared within the membership; (4) review, improve, and model specific protection architectures tailored to security problems present in critical infrastructure industries; and (5) provide a well trained pool of students.

The major research areas that will be supported by the center will be: intrusion detection; attack tolerant networks; denial of service; cyber policy; digital government; and e-commerce; wireless communications and mobile security; and Cryptography. The diversity of resources brought together in the center will facilitate leading edge research in problem areas that require political and legal expertise as well as expertise in security technologies.

We envision that ISEAGE will become an integral part of the CIP and will help enable high quality industrial based research. Members of CIP will receive time on ISEAGE beyond the time used for the research projects.