**Higher Education Information Sharing and Analysis Center (HE-ISAC)**
**Initial High-Level Concept Paper**
**Mark Bruhn**
**1/29/2002**

The development of ISACs was encouraged by Presidential Decision Directive (Clinton PDD 63: Protecting America's Critical Infrastructures), to serve as the "mechanism for gathering of vulnerabilities, threats, intrusions, and anomalies" information from participating institutions, analyzing and developing a recommended response, and disseminating information so that the member institutions can better defend and secure their technology environment and operations. From Executive Order on Critical Infrastructure Protection in the Information Age (October 16, 2001): "The President shall designate a Chair and Vice Chair to enhance the partnership of the public and private sectors in protecting information systems for critical infrastructures and provide reports on this issue to the President, as appropriate; and propose and foster improved cooperation among the ISACS, the NIPC, and other federal government entities."

A current example is the Financial Services ISAC (FS/ISAC), which is exclusively for support of the banking, securities, and insurance industries. Another is the IT-ISAC, which is a not-for-profit corporation serving the information technology industry. ISACs are also in place or planned for the energy, telecommunications, transportation, and Internet Service Provider industries.

Like these industry-specific ISACs, an HE-ISAC would act as the security information collection, analysis, dissemination, and early-warning organization specifically designed to support the unique environment and needs of the higher education community. With information from automated or procedural event "sensors" on member campuses and on national and international research network backbones, incident and activity reports (anonymous or attributed) from members, and with input from and interactions with US Government and law enforcement agencies, technology providers, security associations, other industry ISACs, and subscriptions to vendor and many other security and advisory information services, the HE-ISAC would have a rare aggregate view of the current and near-future security situation in the higher education community.

With this base of data, appropriate synthesis and analytic tools, and access to experienced and expert incident response, security, network and other technology staff (local to the HE-ISAC and through formal arrangements with member institutions), the HE-ISAC would be uniquely positioned to provide early warning about imminent threats with applicable response or self-defense advice, and coordinate a common higher education community response if appropriate. In addition, the HE-ISAC would be a comprehensive source for analysis, information, and guidance on vulnerabilities and solutions, preventative actions, and best practices.

Agility, flexibility, and service related to the needs of the higher-education community would be the goal of the HE-ISAC. No other current organization provides this kind of specific and dedicated support.
Various levels of services can be provided by the HE-ISAC. At the minimal end of the spectrum, the HE-ISAC would coordinate input from established contacts at member institutions and notify member institutions of security alerts. Along the continuum are other activities such as placing sensors on national and even international research networks as well as local member campus networks in order to recognize and warn of attacks or signs of attacks, perform on-campus security assessments, remotely test for possible system vulnerabilities with automated scanning, assist member institutions in responding to security incidents with a trained security team, performing "ethical hacks" to assist member institutions in identifying possible vulnerabilities, and writing white papers and documents related to security issues.

At the ideal service level, the HE-ISAC would be comprised of (see also Figure 1):

Executive Director (1)
Monitoring/Assessment/Reporting Team and Manager (1+6, dependent on initial inputs)
Field Consulting Team and Manager (1+3)
Administration Team and Manager (1+2)
Research Team and Manager (1+3)
Governing/Advisory Committee (comprised of appointees from member institutions)
Ethics/Legal Advisory Committee (comprised of appointees from member institutions)
Technical Advisory Committee (comprised of appointees from member institutions)
Member Representatives (security/liaison contacts at each participating institution)
ISAC Liaisons (contacts at other ISACs)
Organization Liaisons (contacts at CERT/CC, EDUCAUSE, CERIAS, SANS, etc.)
Federal Government Liaisons (contacts at Homeland Security, FBI, NIPC, etc.)

Facilities required would include a 24X7 "war room", with some amount of initial console space and room for expansion as inputs increase. An initial national scope might be segmented over time into monitoring "sectors". Office space for 15-20 would be required, as would budget for equipment, supplies, training, and travel (especially for the Field Consulting Team).

Figure 1 – HE-ISAC Conceptual Organization