Request for Information Comment

Developing a Framework to Reduce the Cybersecurity Risk to Critical Infrastructure

William G. Perry, Ph.D.

Introductory Comments

Institutions of higher education, once a part of the critical national infrastructure, are now absent from the narrative.

Millions of dollars are given to universities to conduct research and development that is related to the nation's critical infrastructure. One example would be research grants focused on the militarily critical technologies list, or MCTL. Another would be nanotechnology. Hundreds of relevant examples would span the nation's entire critical infrastructure.

The information security environment in universities where federally funded research is conducted, may likely be less than robust. Few would argue that information security in institutions of higher learning is strong. The degree of attention given to cybersecurity, however, is as varied as the number of universities that conduct research.

National intelligence services routinely target America's universities with zeal. Limitless vulnerabilities continuously merge with countless threats, and risks are routinely realized. Cybersecurity activities in universities are largely limited to concerns about FERPA (Family Educational Rights and Privacy ACT) and private healthcare information (PHI). Little attention, if any, is given to the unique cybersecurity requirements associated with critical national infrastructure research.

Foreign governments target developing technologies in our institutions of higher education. Congressional reports indicate that American universities are a virtual sieve through which we lose vital research and development. The need to detect and counter the espionage in colleges and universities is obvious.

This commenter has personal experience in working against more than one nation state that was conducting espionage on a college campus. A model for discovering over-the-horizon threats was outlined for law enforcement and the intelligence community.

A core of cybersecurity practices needs to be developed for America's colleges and universities, especially in the area of R&D dollars. The emerging cybersecurity framework should provide for the authority to develop and implement standards that could provide guidance.

I. Current Risk Management Practices

Colleges and universities cybersecurity efforts focus protecting network infrastructure, PHI, FERPA and digital rights. Firewalls are deployed to filter in-bound packets. Employees are educated as to his or her responsibilities under FERPA and PHI. Minimal training of employees is conducted.

INFOSEC policies do exist in many colleges and universities but the relative strength of any cybsersecurity policies and practices tend to be less than robust and vary from institution to institution.

II. Use of Frameworks, Standards, Guidelines and Best Practices

Research would indicate, in the opinion of the commenter, that colleges and universities strive to be in compliance with the non-disclosure elements of HIPPA and FERPA and to have plans in place to protect the infrastructure from malware. The relative strength of information security measures practices, policies and procedures is extremely varied. A framework is absent.

III. Specific Industry Practices

Most colleges and universities function without a comprehensive risk management approach to cybersecurity. The scope of information assurance efforts would include everything from locally generated security practices derived by CIOs and Network Administrators to State Board of Education Policies.

Most colleges and universities strive, as previously mentioned, to be compliant with HIPPA and FERPA. System resiliency practices are gravitating toward off-site background and virtual infrastructure. Some encryption is used.

Stakeholders

The following entities are included as the stakeholders: every privately owned, cross-sector, critical national infrastructure entity, the nation's colleges and universities and state, regional and federal government agencies.

A High Priority Gap

The lack of cybersecurity standards for the administration and secure fulfillment of federal grants in the nation's college and universities is a *high priority gap*. To the best of the commenter's knowledge, there are no standards.

Structured Approach to Risk Management

In the opinion of the commenter, the structured risk based management for cybersecurity isn't followed in the vast majority of universities conducting research related to the critical national infrastructure.

Incentive

The incentive that should be provided to implement a robust cybersecurity framework is that until such a plan is compliant, the flow of federal research dollars would be withheld.

Summary

The level of cybersecurity, as it relates to federal research grant dollars in America's colleges and universities, is weak. Any process to fill the gap would need to include the systematic identification of all federal projects and grants that relate to federal research on the critical national infrastructure.