
**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, DC 20554**

In the Matter Of)
)
Cyber Security Certification Program) **PS Docket No. 10-93**

**COMMENTS OF THE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS OF THE UNITED
STATES, INC.
REGARDING THE PROPOSED CYBER SECURITY CERTIFICATION PROGRAM**

Michael Assante
President and Chief Executive Officer

Kelly Ziegler
Chief Operating Officer

National Board of Information Security
Examiners of the United States, Inc.
2184 Channing Way, #304
Idaho Falls, ID 83404
(208) 557-8026
(973) 860-0921 – facsimile
michael.assante@nbise.org
kelly.ziegler@nbise.org

July 9, 2010

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, DC 20554**

In the Matter Of)
)
Cyber Security Certification Program) **PS Docket No. 10-93**

**COMMENTS OF THE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS OF THE UNITED
STATES, INC.
REGARDING THE PROPOSED CYBER SECURITY CERTIFICATION PROGRAM**

I. INTRODUCTION

The National Board of Information Security Examiners of the United States, Inc. (“NBISE”) appreciates the opportunity to provide these comments in response to the Federal Communications Commission’s (“FCC” or “the Commission”) Notice of Inquiry (“NOI” or “Notice”) on the creation of a Cyber Security Certification Program. In seeking to create such a program, the Commission is making material progress towards addressing what NBISE believes to be one of the greatest challenges facing the United States over the coming twenty years: ensuring the Nation’s information networks are secure and protected from cyber attack, intrusion, and espionage.

The comments that NBISE is submitting in this filing support the Commission’s proposal to create a Cyber Security Certification Program and suggest the Commission include a requirement for personnel certification as part of the Program’s standards. This personnel certification should require information security personnel to demonstrate their ability to apply knowledge, skills, and analytical methods to the conduct of their responsibilities. Such a requirement could include language to the following effect:

Certified entities shall staff positions falling into either of the two categories below with personnel that maintain certification(s) according to a performance-based testing program through which they have demonstrated their understanding of best practices for cyber security and their ability to apply this knowledge to the tasks, responsibilities, and decisions incident to their position:

- Positions that have the primary responsibility, either directly or through communications with others, for the implementation of cyber security best practices.
- Positions directly responsible for complying with Program standards.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to:

Michael Assante
President and Chief Executive Officer

Kelly Ziegler*
Chief Operating Officer

National Board of Information Security
Examiners of the United States, Inc.
2184 Channing Way, #304
Idaho Falls, ID 83404
(208) 557-8026
(973) 860-0921 – facsimile
michael.assante@nbise.org
kelly.ziegler@nbise.org

* Persons to be included on the Commission's service list are indicated with an asterisk.

III. BACKGROUND

NBISE is a newly-created certification body to be formed of dedicated staff and a board of preeminent experts in information security practice and policy. NBISE will develop examinations and certification requirements designed to uphold the highest standards of conduct, professionalism, ethics, and practice in the information security disciplines.

Unlike many commercial certifications available today, NBISE examinations will test candidates' ability to apply knowledge, analytical methods, and acquired skills to achieve desired outcomes. Questions will place candidates in a given circumstance and ensure they are able to properly analyze the situation and respond quickly and accurately to address the issues before them.

The need for such a certification body in the U.S. has been identified by many thought leaders in the Information Security space.¹

Members of NBISE's Council (Board) of Directors are:

- **Franklin Reeder** (Chairman) — Franklin Reeder served at the U.S. Office of Management and Budget for more than 20 years between 1970 and 1995, where he was chief of Information Policy (where he helped develop the Privacy Act of 1974 and the Computer Security Act of 1987), Deputy Associate Director for Veterans Affairs and Personnel, and Assistant Director for General Management. From 1977-80, Mr. Reeder was Deputy Director of House Information Systems, the computers and telecommunications support arm of the U.S. House of Representatives and from 1995-97, he served as Director of the Office of Administration of the Executive Office of the President. He was a member of the Obama-Biden Presidential Transition Team serving on the OMB and White House agency review teams and the technology innovation and government reform team with particular emphasis on the performance and accountability agenda.

¹ See Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Center for Strategic and International Studies. December 2008. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

- **Alan Paller** (Secretary) — Alan Paller is founder and research director of the SANS Institute, a graduate degree granting and research institution with more than 120,000 alumni. He oversees the Internet Storm Center and annual search for the most damaging new attacks. Paller has testified before both the Senate and House. In 2000 President Clinton named him one of the initial members of the President’s National Infrastructure Assurance Council. OMB and the Federal CIO Council named Paller as their 2005 Azimuth Award winner, a singular lifetime achievement award recognizing outstanding service of a non-government person to improving federal information technology.
- **Karen Evans** — Karen Evans presently serves as the National Director for the U.S. Cyber Challenge, the nationwide talent search and skills development program focused specifically on the cyber workforce. Karen was a Presidential Appointee as the Administrator for E-Government and Information Technology at the Office of Management and Budget within the Executive Office of the President. She oversaw the federal IT budget of nearly \$71 billion which included implementation of IT throughout the federal government. Prior to her role as the Administrator, Ms. Evans was the Chief Information Officer for the Department of Energy. Ms. Evans also served as Director, Information Resources Management Division, Office of Justice Programs (OJP), U.S. Department of Justice. She holds a Bachelor’s degree in Chemistry and a Master of Business Administration degree from West Virginia University.
- **James Lewis** — James Andrew Lewis is a senior fellow and Program Director at the Center for Strategic and International Studies, where he writes on technology, security and the international economy. Before joining CSIS, he served at the Departments of State and Commerce as a Foreign Service Officer and as a member of the Senior Executive Service. Lewis has authored more than fifty publications since coming to CSIS and was the Project Director for CSIS’s Commission on Cybersecurity for the 44th Presidency, whose report has been downloaded more than 40,000 times. Lewis received a PhD from the University of Chicago; his current research involves cybersecurity, innovation and economic change; and asymmetric warfare.

- **Richard Schaeffer** — Richard Schaeffer is a widely-recognized leader in information security and national intelligence. A former senior executive with the National Security Agency (NSA), Mr. Schaeffer has over 40 years total U.S. Government service, including 15 years as a member of the Defense Intelligence Senior Executive Service. Principal positions held at NSA include Director, Information and Infrastructure Assurance, in the Office of the Assistant Secretary of Defense at the Pentagon; NSA Deputy Chief of Staff; Acting Director of Research; Director, National Security Operations Center; Information Assurance Deputy Director; and, Information Assurance Director. During the early phase of his career Mr. Schaeffer led technical programs and organizations from several dozen to several hundred people, with financial responsibility from several million to almost a billion dollars.
- **Michael Assante** — Michael Assante is an internationally recognized expert and thought leader in information and cyber security and the recipient of many awards in the space. Mr. Assante most recently held the position of Vice President and Chief Security Officer at the North American Electric Reliability Corporation and oversaw the implementation of cyber security standards across the North American electric power industry. Prior to joining NERC, Assante held notable positions at Idaho National Labs, was Vice President and Chief Security Officer for American Electric Power, and pioneered the security intelligence landscape in his role as Chief Operating Officer of LogiKeep. A former U.S. Navy intelligence officer with experience in information warfare and information security management, Mr. Assante recognized the need to bring intelligence-type analysis to the networks of the corporate world by identifying risks and threats specific to the hardware, software and systems used by individual organizations.

IV. DISCUSSION

The Cyber Security Certification Program the Commission has proposed in its NOI has the potential to create significant value for the public. Teaching consumers to demand higher levels of security from their Internet Service Providers (“ISP”) by providing an identifiable, U.S. Government-sponsored Cyber Security Certification will provide an important incentive for ISPs to adopt best practices and improve their security postures. Much like other consumer-focused programs overseen by the U.S. Government (e.g. the Energy Star program), the proposed Cyber Security Certification Program will help consumers make better choices about their internet service. NBISE strongly supports the development of such a program.

As the Commission considers the details of how such a program will be managed, it is important to keep a critical component of network security in mind. Though the size, configuration, and function of information networks can vary widely, there is a single denominator common to each of them: behind every firewall, system architecture, and vulnerability assessment stands an information security professional. NBISE believes ensuring these individuals are competent, prepared, and capable of making the right decisions day-to-day and during an emergency will be critical to the success of any effort to improve the security of U.S. information networks.

Events such as the Northeast Blackout of 2003 underscore the importance of ensuring qualified professionals build, operate, maintain, and inspect the nation’s critical infrastructure. In this case, as in numerous others, lack of proper training and certification requirements for personnel were found to be a causal factor to this large-scale system failure.² As a result, the Federal Energy Regulatory Commission, through the North American Electric Reliability Corporation, adopted mandatory certification requirements for electric system operators in 2007.³

² Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," U.S.-Canada Power System Outage Task Force, April 5, 2004. <http://www.nerc.com/docs/docs/blackout/ch1-3.pdf>

³ Reliability Standard PER-003-0: Operating Personnel Credentials. Effective date: April 1, 2005. Became Mandatory and Enforceable in the United States on June 18, 2007 through FERC Order 693. <http://www.nerc.com/files/PER-003-0.pdf>

Performance-based certification and licensing requirements for key professionals are common to many specialized professions in the U.S. Neurosurgeons, fighter pilots, and power grid system operators all have one thing in common: they are required to demonstrate their ability to practice their trade with skill and precision prior to being authorized to act without oversight. Demonstrating skill and precision in day-to-day activities, as well as the ability to respond appropriately during an unforeseen emergency, is fundamentally different from reiterating principles and conceptual information. It shows that the individual is competent, prepared, and qualified to become responsible for outcomes of his actions and for the effects they may have on the individuals, controls, and networks under their supervision.

Personnel certification requirements adopted under the FCC-sponsored Cyber Security Certification Program should ensure that the professionals operating information networks are required to demonstrate their ability to not only acquire knowledge, but appropriately apply it to daily and emergency situations. Personnel certification requirements should include acceptable performance on a qualifying performance-based examination combined with specified amounts of work experience and demonstrated adherence to standards of professional conduct.

V. CONCLUSION

NBISE respectfully requests that the commission accept these comments in response to its NOI on the creation of a Cyber Security Certification Program.

Respectfully submitted,

/s/ Michael Assante

Michael Assante
President and Chief Executive Officer

Kelly Ziegler
Chief Operating Officer

National Board of Information Security
Examiners of the United States, Inc.
2184 Channing Way, #304
Idaho Falls, ID 83404
(208) 557-8026
(973) 860-0921 – facsimile
michael.assante@nbise.org
kelly.ziegler@nbise.org