In this fourth article in this five-part series, I look at the controversy surrounding US government proposals for mandatory certification of security professionals.

* * *

On April Fool’s Day 2009, Senators John D. “Jay” Rockefeller (D-WV)<http://rockefeller.senate.gov/> and Olympia Snow (R-ME)<http://snowe.senate.gov/public/> introduced Senate Bill 773<http://thomas.loc.gov/cgi-bin/bdquery/D?d111:1:./temp/~bd2cJW:@@@L&summ2=m&/bss/111search.html>, “A bill to ensure the continued free flow of commerce within the United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes, to provide for the development of a cadre of information technology specialists to improve and maintain effective cybersecurity defenses against disruption, and for other purposes.” The bill’s short title is the “Cybersecurity Act of 2009.”

Among other important proposals bearing on the security of critical communications and computing infrastructure,<http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1354611,00.html> the bill would introduce what Scott Petersen of SearchCompliance.com describes as, “a raft of new federal security standards and certification and licensing requirements that could have major impacts on businesses and security professionals.”


From what I can tell by reading the pro/con arguments, here’s a summary of the arguments. I leave it to readers to make up their own minds.

**Support**

- Other professions involving public safety require government-sanctioned standards and licenses: why shouldn’t critical infrastructure protection?
- Federal government involvement will support nationwide promulgation of better security standards than a hodge-podge of state-government run programs or the chaos of independent standards.
- Defining federal security standards will lend credibility to information assurance and serve as a boost to security awareness.
- Federal standards for the civilian sector will inevitably improve government standards as well.
- Forcing industry to spend money on training and certification will overcome the risk-tolerant, short-term focus on quarterly bottom lines that interferes with rational security management.
Certification would weed out charlatans and incompetents who move from victim to victim as they provide bogus, wasteful, ineffective information assurance advice.

Certification, with its usual requirement for continuing professional education, may support continued learning and adaptation to a changing security environment.

The new law would bring regulatory and legal pressure to bear on the private sector to bring security standards in line with government security standards such as the Federal Information Security Management Act (FISMA).

Legal force would bring the research and standards defined by the National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) Computer Security Division (CSD) to the private sector more strongly.

Testing, certification, and licensing should be removed from organizations that profit from training and education.

All resistance to government involvement in any aspect of business is the mark of either Fascists or devil-worshippers. [OK, it’s joke #1 – it’s an unspoken bias that I suspect is held by some proponents.]

Objections

- Involving government agencies in any aspect of security for a rapidly-evolving high-technology field will slow down people’s ability to respond to changing threats.
- The legislation fails to define the terms “critical infrastructure” and “cybersecurity services” used in defining its mandatory licensing scheme.
- Establishing mandatory training, certification and licensing standards will be difficult and take much longer than the one-year deadline envisaged in the bill.
- Although mandatory certification might be acceptable, mandatory licensing raises much more troubling questions about the nature of the licensing authority, costs, and liability for errors by licensed professionals.
- If licensing is accepted, it must be controlled by state governments, not the federal government, just as other professional licensing is managed.
- The legislation would be expensive and difficult to implement, especially for small-to-medium businesses.
- Unless there are funds allocated for establishing mandatory certification and licensing processes, the bill will be another unfunded or underfunded mandate that will fail because of inadequate planning and resources.
- Mandatory certification requirements may include grandparent clauses that allow incompetent, unqualified personnel to continue in positions of responsibility over information assurance organizations and functions.
- Continuing education requirements for security certifications are too lax to guarantee measurable, real-world growth or even maintenance of professional knowledge and skills in information assurance.
- Compliance with security standards is not in itself a guarantee of improved security.
- Removing competition from testing, certification and licensing will reduce or eliminate free-market pressures for improvement and excellence.
- All government involvement in any aspect of business is the mark of either Communists or devil-worshippers. [OK, it’s joke #2 – it’s an unspoken bias that I suspect is held by some opponents.]

In the next (and last) article, I’ll (finally) respond to a young correspondent’s request for guidance about the “best” security certification for improving job prospects.
For Further Reading


With special thanks to MSIA Prof Paul Brusil, Chief Scientist and Founder of Strategic Management Directions, for several references.

* * *


Copyright © 2010 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.