

[WP-009]

Whitepaper: Critical Infrastructure Certifications

An Observed Discussion of the Introduction of Certified Critical Infrastructure Specialists

Version 050419

April 2005

Author: Bob Radvanovsky, rsradvan@unixworks.com

(A special thanks goes to those listed for being my “sounding board” on this project.)

Copyright © 2005 Bob Radvanovsky. All rights reserved.



Limited Liability Statement

In no event shall the author(s) be liable for any found errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained within this document may be subject to change without any notice. No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this whitepaper.

Documentation pertaining to any security-related technical or proprietary information, its data and all information provided and contained within this document is considered proprietary in nature and subject to copyright protection and is intended solely for use by its owner. Additionally, this documentation is solely for the purposes of discussing a possible, proposed infrastructure issue, and is not dependent upon any specified infrastructure, architectural condition or its issue(s).

No portion of this document is intended to promote, disable, destroy or alter the energy transmission lines at any location, whether within, throughout or out of the United States; instead this paper is intended to identify methods by which will reduce the possible risks associated with the operation of high-tension, high-power transmission lines.

Under the United States Patriot Act of 2001, Title VIII, Section 802(a)(5), no portion of this document is intended to involve activities that:

- (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
- (B) appear to be intended--
 - (i) to intimidate or coerce a civilian population;
 - (ii) to influence the policy of a government by intimidation or coercion; or
 - (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
- (C) occur primarily within the territorial jurisdiction of the United States.

Any such information is intended for “*educational purposes only*”, and is intended solely for the necessary recipients thereof; no other information will be provided that will demonstrate any such acts deemed as “domestic terrorism” under the laws applicable from within the U.S. Patriot Act of 2001.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners. NOTE: Any names not outlined or mentioned above are fictional in nature; as such, any relation to any name or trademark (if any) is purely coincidental.



Introduction

Since September 11 2001, attacks against a structural icon of the United States, The World Trade Center, demonstrated the extent of various vulnerabilities against threat of terrorism. In the aftermath of events, both government and private sector corporations have initiated processes in protecting against any vulnerability that may exist in any of America's critical infrastructures and national key assets. Thus, at all levels, both government and private sector corporations have been stepping up security efforts in securing our national resources.

Addressing any threats that exist within the United States, critical infrastructure industries and operators are assessing their levels of vulnerabilities; they are also increasing their security efforts. Governments from federal down to municipal levels, continue to identify (and where possible, protect) key assets and services within their jurisdictions. Federal departments and agencies are working with critical infrastructure industries to assess key assets and facilitate protective actions (where necessary) while improving the timely exchange of important security-related information through inter-departmental/agency communications channels. In 2002, President George W. Bush signed the Homeland Security Act, which opened a new department: The Department of Homeland Security (DHS). This initiative was a highly aggressive maneuver for the federal government to identify, collecting collaboratively federally controlled departments and agencies, either together under the auspicious of DHS, or cooperatively working through or with DHS. Either way, DHS is now an integral part of the federal government insofar as to risk assessments, mitigation and management at a federal level as well as at several sectors of the critical infrastructure industries. Its sole purpose is an attempt to consolidate intelligence gathering and risk management efforts at a federal level.

In February 2003, the Department of Homeland Security outlined an extensive strategic report entitled "*The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*". This document outlines the importance for securing and preserving critical infrastructure industries as well as key assets of the United States (such as national monuments, icons, statues, nationally-recognized works of art, and key industries that would require continuation of the United States in times of great need). Though the document outlines the perspectives only briefly, the information that it contains is valuable in identifying and outlining the needs nationally in protecting American assets.

Industries classified as "critical infrastructure" from the report are as follows:

- Agriculture and Food
- Water
- Healthcare
- Emergency Services and Management
- Military
- Communications
- Energy
- Transportation
- Money
- Chemical
- Shipping



However, for this document, some industries may be subset to more significant objectives (as outlined below):

Food and Water Production

Food

- Production and Gathering
- Transportation
- Safety

Water

- Reservoir and Resource Utilization
- Treatment
- Recovery

Waste Management and Recycling

- Solid Waste Management (Garbage/Landfill/Incineration)
- Liquid Waste Management (Sewage)
- Recycling

Communications

- Emergency Services and Management
- Military
- Telecommunications (Telephone, TV, Cable)
- Satellite Communications
- Network-Based Communications (Internet)

Energy

Fuel Resource Management

- Nuclear
- Non-Nuclear

Energy Generation

- Nuclear
- Non-Nuclear
 - Coal
 - Hydroelectric
 - Other

Energy Transport (National Power Grid)

Waste Management and Recycling

- Nuclear Waste Management
- Non-Nuclear Waste Management

Transportation

Chemical and/or Hazardous Waste (Non-Nuclear)

Nuclear

Shipping/Cargo

- Air-Based Transport
- Land-Based Transport
 - Rail
 - Truck

Intermodal

Water-Based Transport

Personnel/Consumer

- Air-Based Transport
- Land-Based Transport
 - Rail
 - Bus
- Water-Based Transport

This document will cover those critical infrastructure industries that will require some level of securification, thus this document will provide a guideline for best methods and practices in those industries.



Why Critical Infrastructure is Important to Us

America's critical infrastructure industries provide the foundation for the national security of the United States, its governance, economic vitality, and its way of life. Furthermore, the continued reliability, robustness, and resiliency of these industries define confidence and independence at a national level. Critical infrastructure industries enable the American public to enjoy one of the highest overall standards of living in the world. Their facilities, systems, and functions comprise of environments that are highly sophisticated and complex, as they include human assets, as well as physical and computer-based systems working together in processes that are interdependent of each other. Thus, these environments consist of key functions that, in turn, are essential to the sustained operations of the critical infrastructure industries in which they function.

Key industrial assets, along with national monuments and icons, whose destruction could result in not only large-scale human casualties and destruction of property, would have a profound effect upon human moral, confidence at emotional and psychological levels. Individually, key industrial assets such as nuclear power plants and dams, may not be vital to the continuity of critical services at the national level; however, a combined, successful strike against such targets may result in a significant loss of life and property as well as long-term, adverse public health and safety consequences. Other key assets are symbolically equated with traditional American values and institutions or are affiliated with political and economic establishments. Such values and icons, monuments and historical sites preserve, honor and respect the national history and achievements, while respecting the natural grandeur, of the United States, all of which present targets for individuals or groups of individuals, to commit acts of terrorism.

Individuals who are classified and identified, as "terrorists" are relentless and patient, as evidenced by their persistent targeting of the World Trade Center towers over the years, which eventually paid off. Terrorists are opportunistic, flexible and extremely mobile. These individuals learn from experience, modifying their tactics and targets to exploit perceived vulnerabilities and avoid observed strengths. As efforts increase towards securing predictable targets, these individuals may shift their focus to less protected targets. Enhancing measures and countermeasures for any tactical method or target makes it more likely that they may decide upon another.

Terrorists' pursuit of long-term objectives includes attacks upon critical infrastructures and key industrial assets. Terrorists target critical infrastructures to achieve three general types of effects:

- *Direct infrastructure effects:* Cascading failure disruption or arrest of some functionalities of critical infrastructure industries or their environments, or key industrial assets through direct attacks on a critical node, system, or function.
- *Indirect infrastructure effects:* Cascading failure disruption along with financial consequences for government, social, and economical ramifications through public and private sector reactions from an attack.



- *Exploitation of infrastructure:* Partial failure due to the exploitation of elemental or key parts of a particular infrastructure that disrupts or destroys another target, or infrastructure (may be associated with an indirect attack of another infrastructure or its industry).

What Are the Net-Effect of Acts of Terrorism?

If another act of terrorism were to occur that would involve one (or more) critical infrastructure industries, directly or involved indirectly through another less-critical industry, would (not only) have a profound and significant impact upon that industry, people, businesses and governments that are served by those key industrial assets. This could potentially cripple the United States' ability to function (if affected at a national level) and would:

- Impair the federal government's ability to perform essential national functions.
- Undermine state and local government capacities to maintain order and deliver minimum or essential public services.
- Damage and/or prevent private sector capabilities from maintaining functionality of essential products and services.
- Undermine the public interests and moral at economical and psychological levels.

Where Does Certification Come Into The Equation?

Like any organization that wishes to have their personnel properly educated, ensuring that they are certified ensures a level of understanding. Thus, in the (very) near future, there will begin to emerge certification programs for personnel in key critical infrastructure industries, mostly one that can potentially cripple operations within, throughout and out of the United States. These certifications will vary from broad visional education programs that ensure a fundamental or basic level of understanding, such as security, its concepts, and best practices that may be tailored to specific industries, to highly technical, highly focused, highly specialized certification programs that deal with high risk environments, such as hazardous materials handling procedures of chemical or biochemical waste products. Such certification programs that are that specialized will be very costly, often require very restrictive qualifications, often times requiring serious scrutinized background checks, tests, and personnel evaluations. For those programs that are more broad visional will be far less costly than the specialized programs, and will be tailored to the general base of personnel for more than one industry. These programs will provide 'best practices', and in some circumstances, 'lessons learned' capabilities.

To work at key positions within any company that is classified as a 'critical infrastructure protection industry', may require that their personnel and staff member be trained for fundamental understandings, thus reducing any inherent risks that may be involved with that industry. Such may be a requirement in the near future, esp. industries such as transportation, which will include both hazardous materials hauling, and passenger transportation (air, rail, boat, bus).



The critical infrastructure certification comes as part of a great void which seems to have filled within the security-sectored industry. All in all, there are over 100+ safety and security-related certifications that deal with either safety or security-related issues (there are too many to elaborate, and in my findings, I have found that they are either one or the other, never both). As such, finding a certification that structures the needs of the ‘critical infrastructure protection industry’ revealed only one: CCISP (Certified Critical Infrastructure Security Professional). This certification appears to be sponsored by CIDG Corporation, and focuses entirely on SCADA (Systems Control and Data Acquisition), which are computer-based systems that control much of our infrastructures. SCADA has been repeatedly mentioned many times over the past 4 years within many of the news broadcasts, mostly relating to a catastrophic failure or event, such as the Eastern Coast Seaboard power failure (blackout) that affected several states and major metropolitan areas,, of which hit hardest was New York City.

There is recently, another certification program, called CIPS (Certified Infrastructure Preparedness Specialist), which appears to be pertaining to fundamentals of ‘critical infrastructure protection’, and is based from the NFPA 1600 standard. NFPA 1600 deals (mostly) with incident handling, response and management, along with emergency management and first responder command frameworks. There isn’t much listed about this certification, and I would expect that there is more information about this that will be provided in the very near future.

In my research of all of the various certifications, I have found that of all of the varied security-related ‘clouds’, the one most lacking was the ‘critical infrastructure protection’ cloud. CISSP has general information security covered. MCSE and several of the specialties have the technician, more focused, architecturally-dependent aspects covered. CIFI has forensics management covered, and CISA and CISM have IT auditing and IT auditing management covered. There are a few other off-the-wall specialties, but are so specialized (and probably so technical), that not too many people would use them (or for that matter, know about them). These specialty certifications focus on espionage, hacking, penetration testing and analysis, wireless security, wireless hacking, identity theft, and more.

Conclusion?

I cannot say whether there is, or isn’t a conclusion to this whitepaper – at least, not yet. The ‘critical infrastructure protection industry’ is still very immature, and has several more years to go before reaching a level of understanding that everyone can identify. The biggest problem is trying to explain to people who may not be familiar with the term ‘critical infrastructure’ on what it is or isn’t. For those kinds of challenges, it makes it more difficult convincing people that they need another certification program, focused primarily on fundamental security concepts for ‘critical infrastructure’. When more people begin to understand what and how ‘critical infrastructure’ fit into the larger picture of safety and security, then people will have a greater acceptance for it.

