

[WP-023]

## Whitepaper: Critical Infrastructure Certifications Revisited

An Observed Discussion of the Introduction of Certified Critical Infrastructure Specialists

**Version 050915**

September 2005

Author: Bob Radvanovsky, [rsradvan@unixworks.com](mailto: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 discussing a possible, and/or proposed critical infrastructure protection (CIP) security issues, and is not dependent upon any specified infrastructure, architectural condition or its issue(s). Source information is through observation from previous circumstances, related online documentation, and discussions with colleagues within the security field.

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

---

We have had previous discussions about newly-forming accreditation firms that are establishing themselves as subject-matter experts in the area of “critical infrastructure protection”. Interestingly enough, an observation that I’ve noted has been the definition of this newly-forming “industry” surrounding this concept: “homeland security” versus “critical infrastructure protection”. Depending upon which side of the fence you stand, it can be one or the other, or in some circumstances, both. What I’ve noted is how the terminologies are defined, how they’re used and where they’re utilized.

For the term “homeland security”, implies the protectionist side of the government – that is, it represents the “public sector” of the United States. Having briefly worked for one recently, everything about “critical infrastructure” is lumped under the term/definition of “homeland security”, and is the responsibility of the Department of Homeland Security. Sub-servant departments and agencies are to take their cues and directions from the Central Office of the Department of Homeland Security, located in Washington, D.C. Essentially, insofar as to how the governments (federal, state, county and local) view “homeland security” is more so from the perception of “first responder”, which many of you have heard that term used during the aftermath of the Hurricane Katrina disaster relief efforts. So what is a “first responder”?



## First responder

---

The term “first responder” refers to those individuals who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101), as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) that provide immediate support services during prevention, response, and recovery operations.<sup>1</sup> So this pertains to what used to be called “emergency preparedness”, right?

First responders can be law enforcement (police), fire protection (firemen), paramedics, first aid, EMTs (EMT means “emergency medical technician”<sup>2</sup>, which some might confuse with a “paramedic” – to me, they appear as one and the same, with one slight difference: usually a paramedic is associated with a fire department or ambulatory care department; EMT might not be), and (of course) government officials. To me, this truncates the definition from the term “first aid responders” from earlier years (having recalled my days in Boy Scouts and first aid conferences). First responders provide medical, evacuation management (now called “incident command management”), food and water, shelter, and communications.

## A “widget” by any other name...

---

So we come to the definition of “critical infrastructure protection” versus “homeland security”. CIP focuses on proactively protecting our national infrastructures (see “*Whitepaper: [WP-009]: Critical Infrastructure Certifications*”), while homeland security deals with (mostly) response. There ARE some differences, but much depends on how you want to address a crisis. If you are considered a “first responder” your emphasis will be treating victims of man-made and natural disasters; if a CIP specialist your emphasis will be relating more towards risk assessment and management. Clearly, there are some differences.

The interesting thing about these two (2) definitions are their interrelation to each other – one cannot exist without the other, and both serve and provide unique and protecting measures towards safeguarding people, structures and information. CIP cannot exist solely as a reactive measure to homeland security, and homeland security cannot exist without some preventative measure or countermeasure to be taken. Both rely heavily on each other, as well as the coordinated efforts of efficient management, effective communications and coordinated deployment and remediation efforts.

To the average individual who has heard these terms interchangeably used, they are incorrect – there IS a difference. Yet, these individuals and organizations continue to utilize them in a manner which confuses people who want to either help during/after a disaster, or make a career/professional change in their lives.

---

<sup>1</sup> <http://www.piercecountywa.org/pc/abtus/ourorg/dem/DefineFirstResponder.htm>.

<sup>2</sup> <http://www.answers.com/topic/emergency-medical-technician>.



Here is where the certifications come into existence. The certifications that exist now, and in the years ahead) focus on clarifying on these aspects from both worlds. Also, additional, more specialized certifications will emerge, especially tailored towards specifics of one given sector (as listed of the now 18 sectors within HSPD-7), or its aspect (such as an industry that serves that sector). Either way, there will be an increasing need for training and certifying those individuals who work within and/or service those sectors.

## **I'll have my cheeseburger with onions, please**

---

So what certifications exist out there relating to either “homeland security” or “critical infrastructure protection”? Actually, quite a few – they are categorized by area of specialty and range from generalist to specialist. There are a few that specifically mention either the words “homeland”, “security” or “critical infrastructure” in the title of the certification; whether or not these have any significance is what’s important.

From the generalist, non-specific certifications, there appears to be several:

***Certified Infrastructure Preparedness Specialist (CIPS)***  
***Certified in Homeland Security (CHS)***

For the CIPS certification, this is offered by a group from the Office of Infrastructure Preparedness<sup>3</sup>, which appears to offer more direction towards emergency preparedness, regulatory and governance, and risk management.

For the CHS certification, this is offered through the American College of Forensics Examiners Institute (ACFEI) of Forensics Science<sup>4</sup>, which appears to offer more direction towards law enforcement and governance.

From the specialist, very specific certifications, there appears to be several:

***Certified Critical Infrastructure Security Professional (CCISP)***  
***Certified Information Systems Security Professional (CISSP)***  
***Certified Information Security Manager (CISM)***  
***Certified Information Security Auditor (CISA)***  
***Certified Information Forensics Investigator (CIFI)***  
***Certified Business Continuity Professional (CBCP)***  
***Certified Fraud Examiner (CFE)***  
***Certified Protection Professional (CPP)***

---

<sup>3</sup> <http://www.oip-usa.us/cips.html>.

<sup>4</sup> [http://www.acfei.com/certification\\_programs-chs.php](http://www.acfei.com/certification_programs-chs.php).



Not to be confused with the Certified Information Systems Security Professional (CISSP) from (ISC)<sup>2</sup>, the CCISP, is sponsored by the Critical Infrastructure Institute<sup>5</sup> and focuses mostly on control systems. Control systems make up part of SCADA (Supervisory Control and Data Acquisition), which (pretty much) RUN this country: gas pipelines, electrical grid for the entire nation, telecommunications networks, HVAC systems, etc.

The Certified Information Systems Security Professional (CISSP)<sup>6</sup> offered through (ISC)<sup>2</sup> has (for years) been the “de facto” security certification, which covers just about every aspect of security, but focuses mostly on Information Technology security.

The Certified Information Security Manager (CISM) by the Information Systems Audit and Control Association (ISACA)<sup>7</sup> appears to be a similar version to that of the CISSP, but focuses more on the auditing aspects of security, instead of all aspects of security.

The Certified Information Systems Auditor (CISA), also by ISACA, is a specialty certified IT auditor certification. The CISM would be the managing individual over the department utilizing the auditors.

The Certified Information Forensics Investigator (CIFI) offered through the International Information Systems Forensics Association (IISFA)<sup>8</sup>, and focuses on Information Technology forensics, looking for “breadcrumbs” and other traceable information specific to IT-related investigations.

The Certified Business Continuity Professional (CBCP) by DRI International<sup>9</sup> focuses on certifying business management professionals who make efforts of ensuring continued operations. This focus is mostly on disaster recovery planning, risk mitigation and risk management.

The Certified fraud Examiner (CFE) by the Association of Certified Fraud Examiners<sup>10</sup> appears to be another specialty certified examiner, similar to the CIFI certification, but is more broad-based and covers law enforcement, all forms of forensics and private investigation techniques.

The last certification which might be considered a critical infrastructure certification is the Certified Protection Professional (CPP) offered by ASIS<sup>11</sup> appears to focus primarily around law enforcement.

---

<sup>5</sup> <http://www.ccispcert.com/about.htm>.

<sup>6</sup> <https://www.isc2.org/cgi-bin/content.cgi?category=97>.

<sup>7</sup> <http://www.isaca.org>.

<sup>8</sup> <http://www.iisfa.org>.

<sup>9</sup> <http://www.drii.org>.

<sup>10</sup> <http://www.cfenet.com/home.asp>.

<sup>11</sup> <http://www.asisonline.org/certification/cpp/index.xml>.



## How do CIP/HS certifications have significance?

---

This is an emerging industry, and I foresee that it will mature nicely over the next several years. In the meantime, expect to see more specialty certifications, perhaps in some of the more critical sectors that make up the 15 or so “critical infrastructure” sectors. Each certification listed above and on previous pages has significance in that it:

- registers those who are knowledgeable in areas of expertise
- provides certified or trained operations continuity managers, electrical and mechanical systems planners and designers, and categorical specialists
- ensures consistency within the industry, its terminology and definitions, and what is to be expected within the industry, and;
- determines location, purpose, function and extent of infrastructure and its interactions with neighboring infrastructures, services and environments.

CIP/HS isn't an easy thing to figure out. It's complex, and has interdependencies upon interdependencies both within and between each sector (or multiples thereof). CIP/HS is an encompassment of both wide-angled and narrow-angled lenses on the same sector, as one sector can (potentially) have a devastating impact on other sectors and industries. Therefore, the need for ensuring that qualified individuals know this material – cold – is important.

As a side note about the certifications, many of these existed well before the circumstances that developed resulting from the 9/11 incident at the World Trade Center Complex in New York City; however, three (3) stands out the most significantly, such that these are specifically tailored towards CIP/HS:

- ***Certified Infrastructure Preparedness Specialist (CIPS)***
- ***Certified in Homeland Security (CHS)***
- ***Certified Critical Infrastructure Security Professional (CCISP)***

The two (2) generalist certifications focus on important aspects of emergency preparedness, risk management, regulations and governance. Knowing the laws and their regulations are important, esp. if performing a risk assessment at a site. The last one I find equally important based on the fact that not too many people realize, is the significance of SCADA, and just how vital it is to our country. Without it, oil and gas wouldn't flow, water wouldn't flow, waste wouldn't be taken from our homes, buildings wouldn't get heated in the winter and cooled in the summer, and communications links would go down. SCADA is a sensitive and touchy area in that it affects industrial and government standards alike, both current and emerging, within the United States and abroad. Expect to see more standardized communications protocols specifically aimed and defined towards SCADA in the years to come. The federal government has invested quite a bit of money in SCADA research. This being said, expect to see much more information and security awareness training and certification programs offered through both private and government-sponsored events.

